DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
2300/05B
CP

From: Commandant of the Marine Corps

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT CHANGE MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-05B Enterprise Information Technology Service Management Change Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Change Management Process Guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity.

2. CANCELLATION. 2300-05A.

3. AUTHORITY. The information promulgated in this publication is based upon policy and guidance contained in reference (a).

4. APPLICABILITY. This publication is applicable to the Marine Corps Total Force.

5. SCOPE.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the Director, Command, Control, Communications and Computers.

6. SPONSOR. The sponsor of this technical publication is HQMC C4 CP.

K. J. NALLY
Brigadier General
U.S. Marine Corps
Director, Command, Control,
Communications and Computers (C4)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

DISTRIBUTION: PCN 18623000500

Enterprise IT Service Management
Change Management
Process Guide

Release Date:
4 August 2014

Document Approval / Major Revision Change History Record

This table is used for initial release and subsequent revisions. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions are required when the intent or process is changed rendering the prior version obsolete or when the number of minor releases total twenty (20). Changes to this document shall be recorded, described, and approved using the table below:

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	Process Owner/Approver	
09/21/09	0.1			Draft Release
		Printed Name	Printed Name	
11/24/09	1.0			Initial Release
		Printed Name	Printed Name	
06/18/10	2.0			Updated as per CRMs from the follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
08/24/10	3.0			Updated as per CRMs from the follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
12/17/10	4.0			Updated as per CRMs from the follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
02/17/11	5.0			Updated as per CRMs from the follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
04/14/11	6.0			Updated as per CRMs from the follow-on E-ITSM Task Order, CDRL L3003
		Printed Name	Printed Name	
06/06/11	7.0			Updated as per CRMs from follow-on E-ITSM Task Order CDRL L3003
		Printed Name	Printed Name	
04/05/13	8.0			Quarterly Process Owner Updates per C4 MCATS Tasker
		Printed Name	Printed Name	
06/27/14	9.0			Process Owner Updates
		Printed Name	Printed Name	
08/04/14	10.0		Scott Kellen	Updated as per CRMs from Process Owner Updates
		Printed Name	Printed Name	

Table of Contents

List of Tables

List of Figures

1.0 INTRODUCTION

1.1 Purpose

The purpose of this process guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC IT activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity as represented in Figure 1.

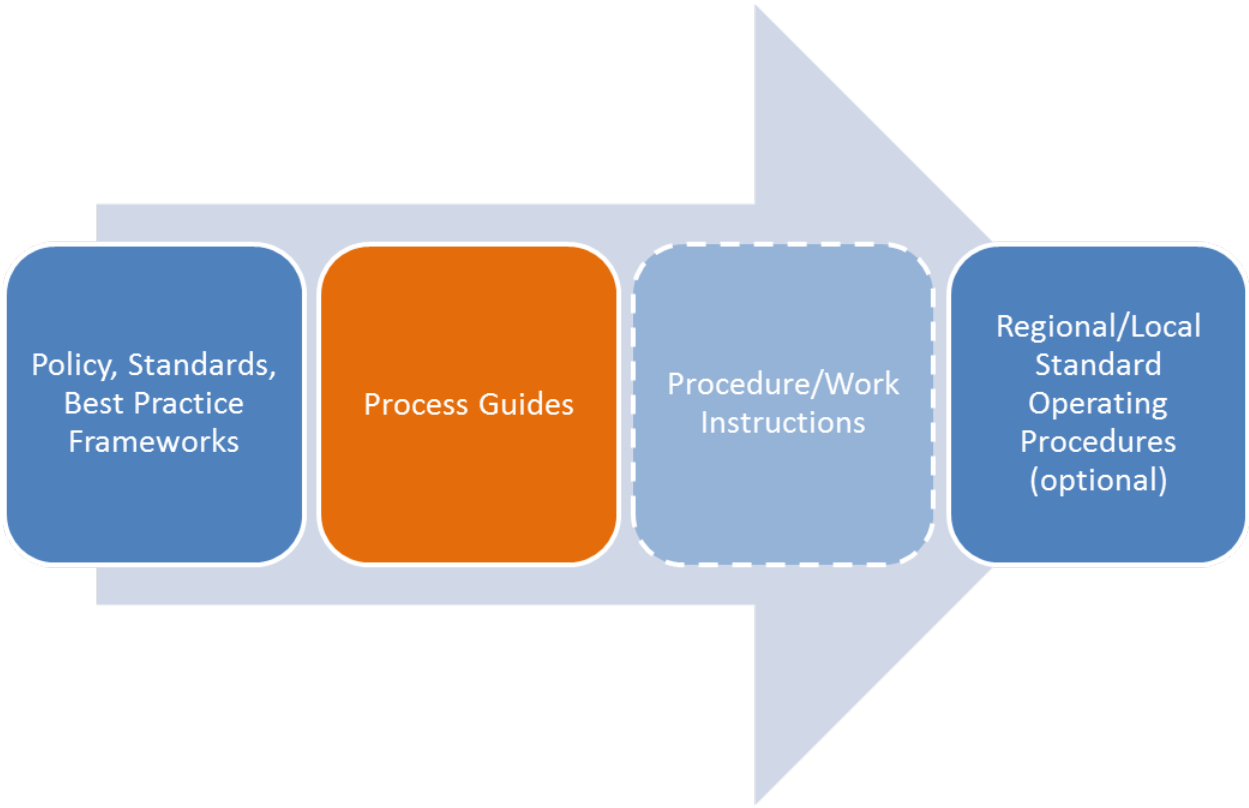


Figure 1. Document Process Continuum

1.2 Scope

The scope of this document covers all services provided in support of the MCEN for both the Secret Internet Protocol Router Network (SIPRNET), and the Non-Secure Internet Protocol Router Network (NIPRNET). Information remains relevant for the global operations and defense of the MCEN as managed by Marine Corps Network Operations and Security Center (MCNOSC) including all Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation (MCI) commands.

Table 1 depicts the various layers of document design. Each layer has discrete entities, each with their own specific authority when it comes to promulgating documentation. This enterprise process operates at Level B, sub processes such as procedures and work instructions are not included within the scope of this document.

Table 1. Document Design Layers

	ENTITIES	DOCUMENTS GENERATED
LEVEL A	Federal Govt DoD DoN CMC/HQMC	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	HQMC C4 MCNOSC MCSC	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	RNOSC MITSC	Regional Procedures Work Instructions
LEVEL D	MCBs POSTS STATIONS	Locally Generated SOP's

1.3 Document and Process Change Procedures

This document will be reviewed semi-annually for accuracy by the Process Owner with designated team members. Questions pertaining to the conduct of the process should be directed to the Process Owner. Suggested Changes to the process should be directed to USMC C4 CP in accordance with MCO 5271.1B Information Resource Management (IRM) Standards and Guidelines Program.

2.0 PROCESS OVERVIEW

2.1 Purpose, Goals, and Objectives

The goal of the Change Management (ChM) process is to facilitate the successful introduction of changes within the IT environment. The process also ensures that appropriate details of changes to Configuration Items (CI) are recorded.

Objectives of ChM include:

Controlling IT infrastructure changes through standardized, repeatable methods and procedures

Verification and validation of changes

Supporting the efficient handling of changes

Providing accurate, timely information on changes

Minimizing the impact of changes on operating forces and garrison commands

Reducing Incidents caused by changes

Providing accurate assessment of the cost of proposed changes before they are incurred

Providing an enhanced perception of the quality of IT

Providing change documentation to reflect all changes that will be implemented—before the change is actually implemented

This process guide addresses changes to both the Operational baseline and the Service Design baseline. Changes to the Service Design baseline are those that will impact the design of enterprise services requiring strict adherence to the Technical Design Life Cycle (TDLC) process. Service Design changes always change the Operational baseline; however, Operational changes do not change the Service Design baseline. All approved changes, whether they impact operational baselines or design baselines require documentation and are controlled through one oi several Change Management or Change Approval Boards. Examples of Operational baseline changes would be a break-fix, various types of rule changes (ACL, firewall, etc.), and end-user support. Examples of Service Design baseline changes would include; a product change (e.g., hardware or appliance changes to new models/manufacturers), software procurements not previously released within the enterprise that is not in the USMC Service Catalog. An example of a situation where the operational baseline may change prior to the service design baseline changing is an IAVA.

2.2 Relationships with other Processes

All IT Service Management processes are interrelated. The Processes in Figure 2 were selected due to the strength of the relationships and dependencies between them and the degree to which they underpin USMC near-term objectives. While any one of the processes can operate in the presence of an immature process, the efficiency and effectiveness of each is greatly enhanced by the maturity and integration of all processes. Figure 2 depicts key relationships that exist

between ChM and the other processes. This figure is not all-encompassing and the relationships shown can be direct or indirect.

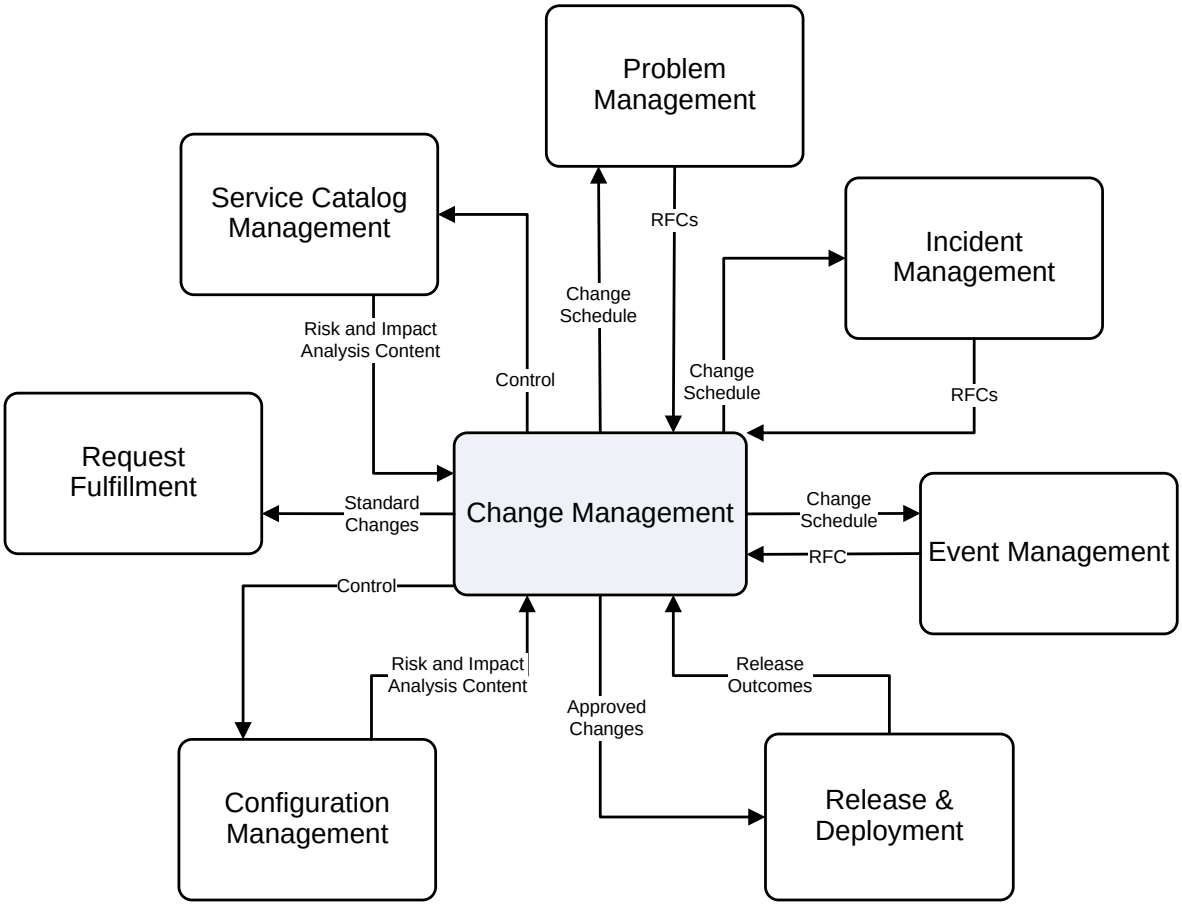


Figure 2. ChM Relationship with other Processes

The following list describes the ChM relationship (input or output) to other Processes, as depicted in the Figure 2:

Service Catalog Management

- Control: The Service Catalog's value is dependent on the accuracy of its content. Effective coordination between ChM and Service Catalog Management (SCM) is required to ensure that every Request for Change (RFC) is analyzed for impact to the Service Catalog. As changes that result in material changes to service catalog content are released into production, the Service Catalog is updated accordingly.
- Risk and Impact Analysis Content: The Service Catalog is the definitive source of record for services that are present in the Configuration Management Database (CMDB) and can provide rapid, at-a-glance views into key service attributes to

include availability targets, maintenance windows, and change freeze periods for the purposes of change evaluation and planning.

Incident Management

- Change Schedule: The Change Schedule is a valuable tool for the Service Desk and other key Incident Management process stakeholders for the purposes of initial diagnosis and troubleshooting. Determining "what changed?" is on the critical path to rapid restoration of service. The Change Schedule can provide quick, valuable insight into this activity.
- RFCs: Some incidents will require an RFC to execute corrective actions and restore service.

Event Management

- Change Schedule: Event Management (EM) utilizes the Change Schedule to prepare for the potential need to suspend and resume monitoring and EM activities associated with changes that impact any service attributes being monitored (e.g., availability, performance, capacity, etc.).
- RFC: EM will identify qualified events that do not result in an Incident but do require an RFC prior to execution of corrective action. For example, an unauthorized CI or a non-standard configuration may trigger an alert and require an authorized RFC prior to execution of corrective action.

Release and Deployment Management

- Authorized Changes: Release Management awaits authorization of RFCs prior to deployment. Beyond triggering authorization, the RFC includes key directives such as approved deployment windows to which Release Management adheres.
- Release Outcomes: The Change Management process does not "end" for an RFC upon authorization. Rather, Release Management provides Change Management with key outcomes, such as actuals for deployment start/end, results of post release testing, and any Incidents encountered. This information is used by Change Management to determine any further actions, to include initiation of a Post Implementation Review (PIR) or closure of the RFC(s).

Configuration Management

- Risk and Impact Analysis Content: The CMS depicts relationships between services and CIs, enabling risk and impact analysis for the purposes of Request for Change (RFC) evaluation.
- Control: To keep information current, CI data and history is updated both by ChM to Configuration Management (CfM) and vice versa. Configuration Management provides the infrastructure data required to assess Customer impact of an IT infrastructure component failure and aids identification of the CI Owners and

associated User(s). Status of Changes, especially completion, is an input to CfM keeping the CMDB current.

Problem Management

- Change Schedule: The Change Schedule is a valuable tool for the Service Desk and other key Incident Management process stakeholders for the purposes of initial diagnosis and troubleshooting. Determining "what changed?" is on the critical path to rapid restoration of service. The Change Schedule can provide quick, valuable insight into this activity.

- RFCs: Problem will require an RFC to correct the root cause of known errors.

Request Fulfillment

- Approved Standard Changes: ChM routes Requests For Change (RFC) to Request Fulfillment when it is determined within ChM that an RFC can be processed as a standard change. ChM also provides RqF with specifics related to the defined CAB approved standard changes.

2.3 High-Level Process Model

The ChM process consists of seven (7) distinct sub-processes and is integrated with the Release and Deployment Management (RDM) and CfM processes. The following workflow depicts these processes and sub-processes that collectively enable and underpin ChM. See Section 4.0 for complete descriptions of the sub-process activities.

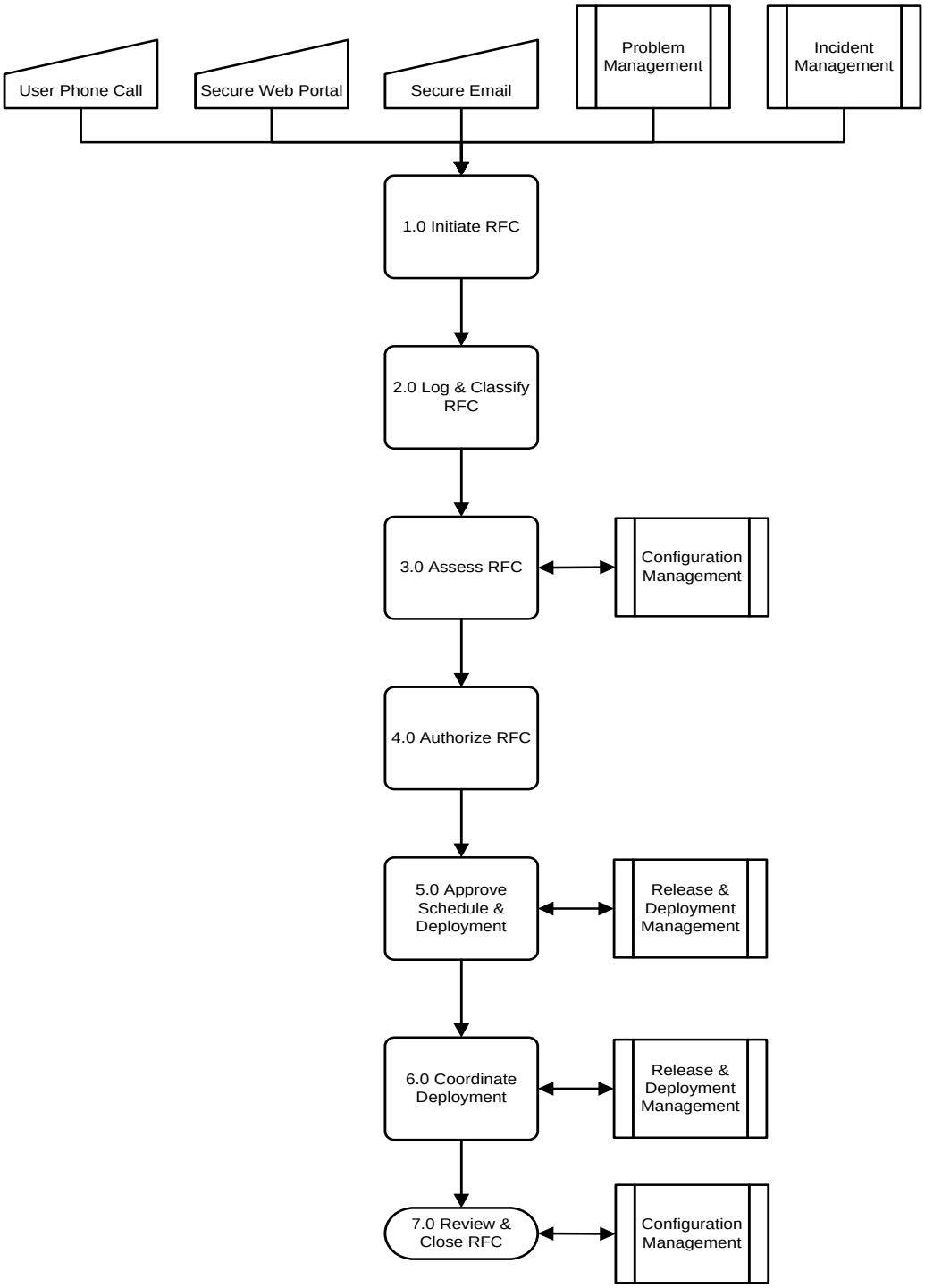


Figure 3. High-Level ChM Workflow

Table 2 contains descriptions of each sub-process. Each sub-process number is hyperlinked to its detailed description in Section 4.0, Sub-Processes.

Table 2. ChM Process Activity Descriptions

Number	Process Activity	Description
1.0	Initiate RFC	An RFC is submitted via the Enterprise Change Management tool (currently Remedy), triggering the ChM process. Roles that may submit an RFC: At the enterprise level RFCs are created by project officers. At the regional level and below RFCs are created by technical sections, IAMs, etc. RFCs may also result from the Incident and Problem Management processes.
2.0	Log & Classify RFC	Includes setting impact, urgency, risk and type of change, etc. This helps to appropriately route and record the RFC and facilitate the subsequent review and authorization process.
3.0	Assess RFC	Review the RFC for completeness and accuracy. RFCs that fall outside the Area of Responsibility (AOR) or are otherwise incomplete or inaccurate are returned with a rationale for denial. The change authority is determined by RFC type, classification, and/or Change Manager discretion.
4.0	Authorize RFC	Determines the disposition of a change, including review of pertinent information, by the change authority as designated by the organization, examples include CO, Operations Officer, Change Advisory Board, Change Manager, etc. Designation will be determined by the type, risk, complexity and impact of the change. Note that not all RFCs require CAB approval (i.e. standard change).
5.0	Approve Schedule and Deployment	The appropriate change authority, as determined by the category of the change, approves the deployment of the change after reviewing the implementation plan with RDM (as required). The focus of this step is ensuring the deployment schedule adheres to any maintenance window or freeze periods and does not interfere with other scheduled changes. Note that approval of a change for deployment is separate from change authorization, which occurs earlier in the process.
6.0	Coordinate Deployment	Ensure the change is implemented as specified by reviewing all deployment updates and notifications received from the deployment team to ensure the deployment is in compliance with the approved RFC. Act on deployment team feedback as needed to protect the integrity of the IT environment.
7.0	Review and Close RFC	This activity ensures change records are reviewed with the customer, closed and recorded. Post Implementation Reviews (PIR) optimize efficiency and effectiveness by identifying service and process improvement opportunities.

2.3.1 Process Description

Changes are made for a variety of reasons and in different ways – for example:

- Proactively, e.g. reducing costs, improving services, or increasing ease and effectiveness of support
- Reactively as a means of resolving errors and adapting to changing circumstances.

Changes should be managed in order to:

- Ensure that all stakeholders receive appropriate and timely communication about the change so that they are aware and ready to adopt and support the change
- Minimize the impact and disruption
- Optimize risk exposure
- Achieve success on the first attempt.

2.3.1.1 ChM Process Integration with the Acquisition Life Cycle

The Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System provides a thorough workflow model from the Materiel Solution Analysis Phase through the Operations & Support phase. The Joint Capabilities Integration & Development System (JCIDS) is a procedure that helps generate and define requirements based upon capabilities as requested or defined by all four DoD military services, including the USMC; JCIDS is an integral part of the Life Cycle Management System.

Service Portfolio Management through integration with the enterprise ChM process, introduces new systems into the production environment and provides lifecycle support on existing systems. As potential configuration items, these systems and their integrated components are subject to change management as they are being fielded within the operational environment. Systems that are enterprise in nature (as evidenced within the enterprise Service Catalog) are subject to change control as provided by the enterprise ChM process. Figure 4 provides an overview of this integrated structure for service design.

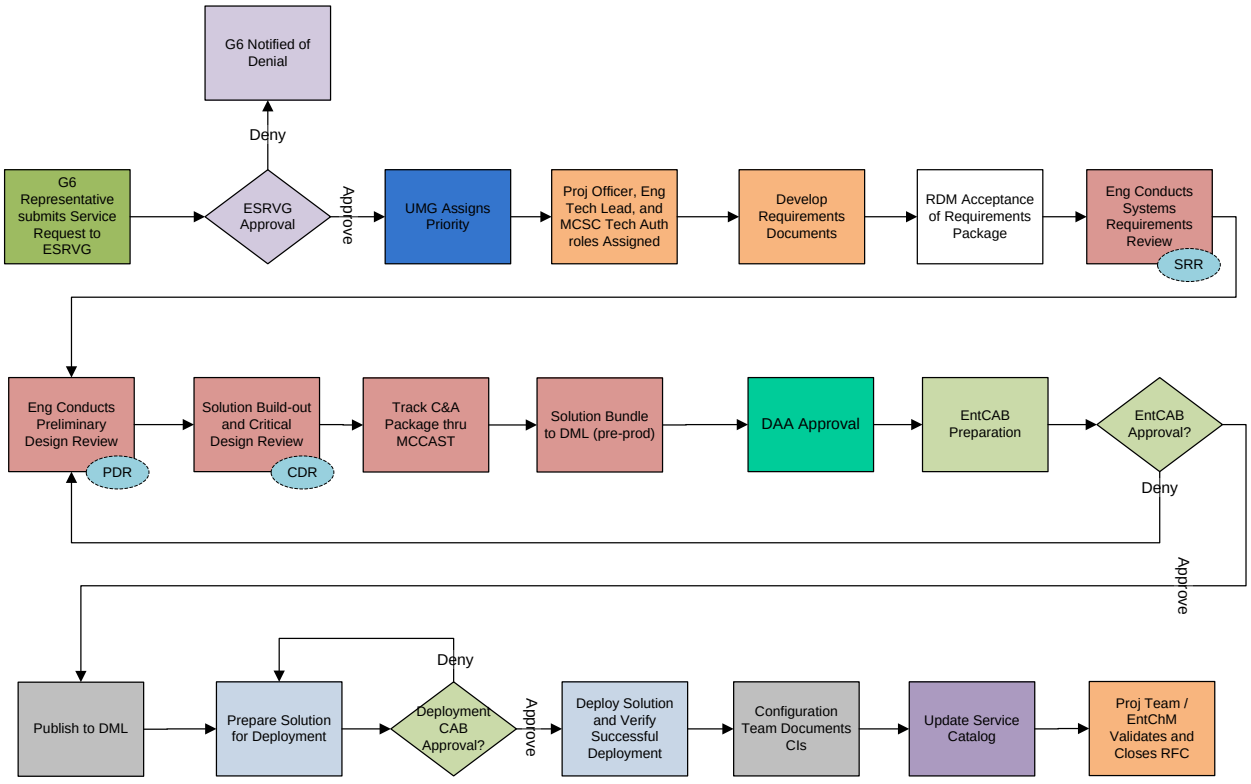


Figure 4. ChM and Acquisition Conceptual Integration

2.3.1.2 RFC Flow

Figure 5 illustrates the standard routing of RFCs from the Change Requester to process termination.

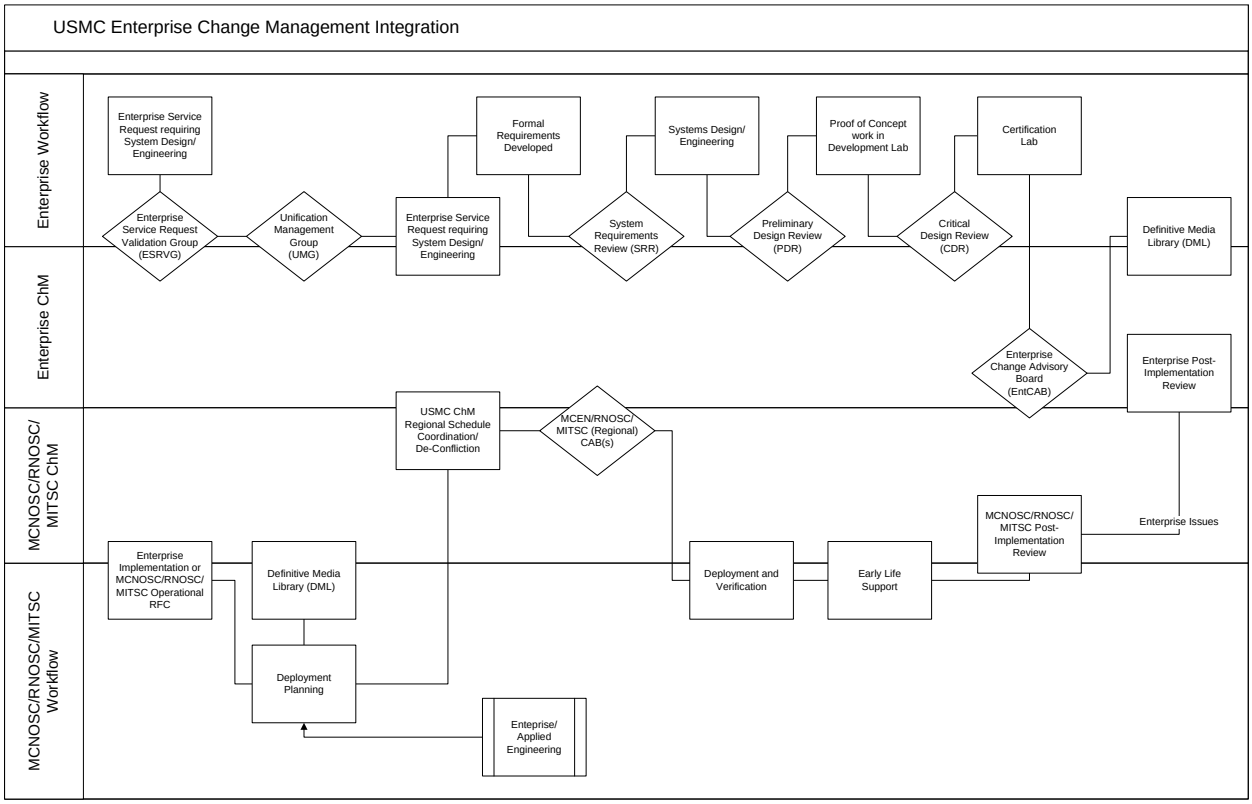


Figure 5. ChM RFC Flow

2.3.1.3 USMC Change Advisory Board Structure

The USMC Enterprise Change Advisory Board (EntCAB) is the body that exists to support the authorization of changes and to assist change management in the assessment, prioritization and scheduling of enterprise changes. The EntCAB is the change authority for many change categories, but for some changes the EntCAB will act in an advisory role. There are also Regional CABs (RCAB) that are responsible for changes within their AOR. It is important that each CAB has full visibility of all changes that could have an impact on the services and configuration items within its AOR.

Enterprise CAB: The EntCAB provides decisions on new or modified enterprise service designs to be published to the Definitive Media Library. As such, the EntCAB reviews changes that impact enterprise service design baselines.

Regional: Regional (RNOSC/MITSC) CABs review RFCs submitted by users within their respective commands or programs, and those RFCs forwarded by local Change Managers within their area of responsibility. When the Regional CAB determines an RFC has a potential enterprise impact, the RFC is submitted to the EntCAB for review.

Communication between CAB levels is accomplished by Change Coordinators; within local ChM processes, the Change Manager may serve as the Change Coordinator where appropriate.

2.3.1.3.1 EntCAB Membership

EntCAB membership is comprised of Standing and Invited members. Standing members constitute the Core Team; these representatives, including the enterprise Change Manager, have permanent representation on the EntCAB. Invited members constitute the Dynamic Team; these persons are invited at the behest of the Change Manager in accordance with the type and scope of RFCs being reviewed.

The members depicted on Figure 6 represent *functional* coverage, not specific billets or resources. When appropriate, the Change Manager may excuse certain core members from attendance. For example, if certain administrative functions have already been reviewed for an RFC at the Regional level, representation of those functions is not required during the enterprise review.

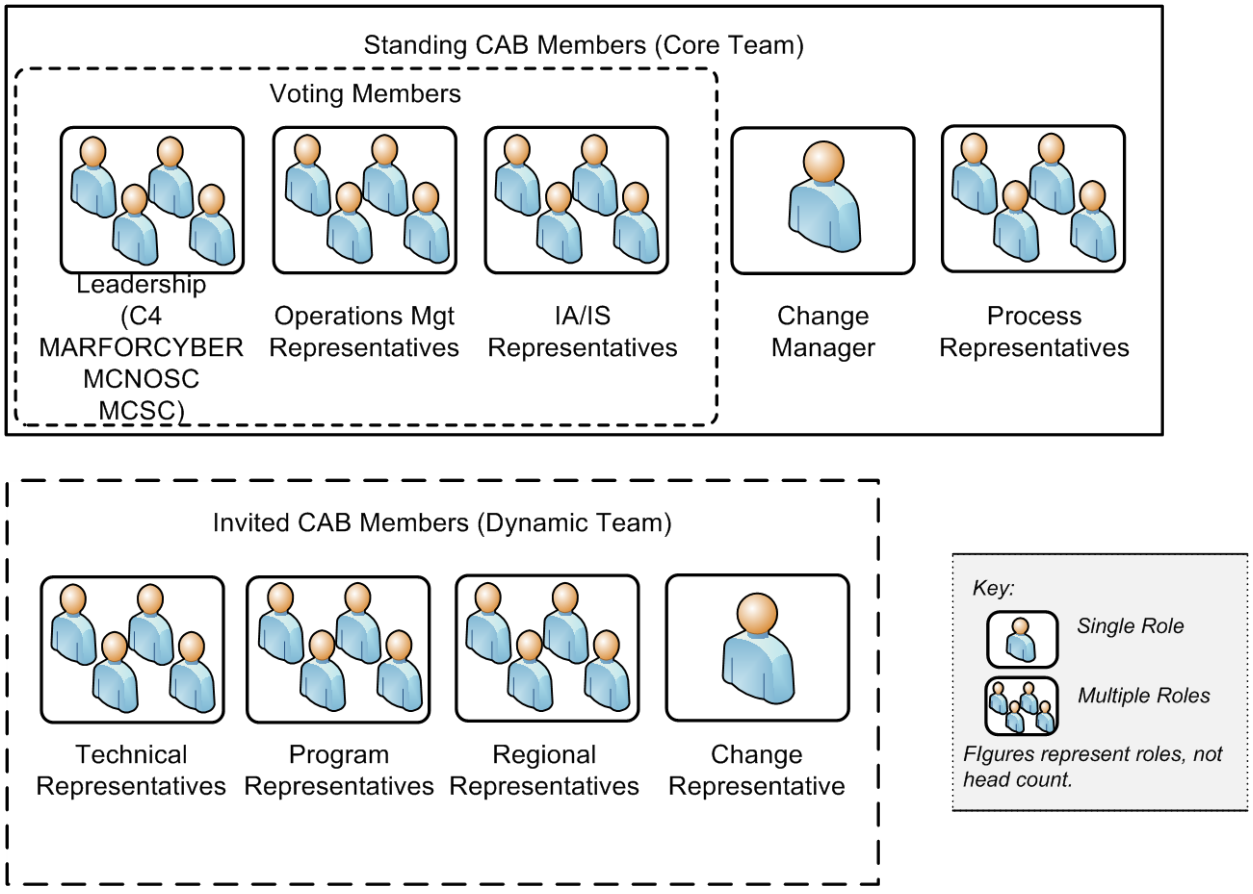


Figure 6. CAB Functional Membership Representation

2.4 Key Concepts

ChM relevant key concepts are described below:

2.4.1 Change

The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items. Examples of changes include the addition, modification, or removal of approved, supported, or baselined hardware, network infrastructure, software, application, environment (HVAC, power, etc.), system, desktop build, or associated documentation.

2.4.2 Change Advisory Board

The CAB is a select group (including representatives from IT and the business) with the change authority for significant changes. Significant changes are characterized as having complex or considerable impact and/or build or runtime required resources.

2.4.3 Change Evaluation

Change Evaluation provides a consistent and standardized means of predicting performance of a service change in the context of existing and proposed services and IT infrastructure. Then the actual performance of a change is assessed against its predicted performance and any deviations between the two are understood and managed.

2.4.4 Change Model

A Change Model provides a repeatable way of dealing with a particular category of change and defines specific steps that will be followed for a change in this category. Change Models may be simple (i.e., a Standard Change) or they may be very complex.

2.4.5 Change Proposal

Change proposals are submitted to change management before chartering new or changed services in order to ensure that potential conflicts for resources or other issues are identified. A Change Proposal includes:

- A high-level description of the new, changed or retired service, including business outcomes to be supported, and utility and warranty to be provided.
- A full business case including risks, issues and alternatives, as well as budget and financial expectations.
- An outline schedule for design and implementation of the change.

2.4.6 Change Record

A record containing the details of a change. Each change record documents the lifecycle of a single change. A change record is created for every request for change that is received. Change records should reference the configuration items that are affected by the change.

2.4.7 Change Request or Request for Change

A Change Request or Request For Change (RFC) is a means of formally proposing changes. A Change Request includes details of the proposed change. The term RFC is often misused to mean a change record, or the change itself.

2.4.8 Critical Success Factors

Critical Success Factors are elements, items or activities required to ensure success of the mission.

2.4.9 Emergency CAB

Emergency CAB (ECAB) meetings are convened to facilitate emergency changes. The ChM process is still followed, albeit certain activities may have to occur retroactive to deployment. The Emergency CAB is a subset of each CAB in the overall USMC CAB structure, which allows emergency RFC decisioning to occur by an individual or smaller component of the overall CAB membership. RFCs are declared emergencies at the recommendation of the Change Requester or Change Advocate, and upon concurrence with either the Change Manager or Watch Officer on behalf of the Change Manager.

2.4.10 Emergency Change

An Emergency Change is used to restore service due to an outage, impending outage, or significant degradation of service. An Emergency Change is never used for new or modified services. For high priority and/or urgent new or modified services an expedited normal change should be used.

2.4.11 Key Performance Indicators

Key Performance Indicators are measures or metrics of progress toward meeting a Critical Success Factor within a process, project, plan or IT service.

2.4.12 Post-Implementation Review

A Post Implementation Review is a structured and exhaustive review that occurs for specific changes. A Post Implementation Review is generally conducted for changes that either failed or were problematic. A Post Implementation Review is an activity found within the *Review and Close RFC* sub-process and is distinct from a Change Review. Post Implementation Reviews may occur several months after an RFC has been closed.

2.4.13 Service

A Service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. Services facilitate outcomes by enhancing the performance of associated tasks and reducing the effect of constraints.

2.4.14 Service Management

Service Management is a set of specialized organizational capabilities for providing value in the form of services. Service Management takes the form of a set of functions and processes for managing services over their lifecycle. It is the means by which services are monitored and controled on a day-to-day basis.

2.4.15 Service Transition

Service Transition ensures that new , modified, or retired services meet the expectations of the business as documented in the service strategy and service design stages of the life cycle.

2.5 Quality Control

2.5.1 Metrics, Measurements and Continual Process Improvement

Continual Service Improvement (CSI) depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process at hand. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measures of how well the process is working, whether or not the process is continuing to improve, or where improvements should be made. When evaluating process metrics, the level of improvement is more important than the magnitude of the metric.

Effective day-to-day operation and long-term management of the process requires the use of metrics and measurements. Reports need to be defined, executed, and distributed to enable the managing of process-related issues and initiatives. Daily management occurs at the process manager level. Long-term trending analysis and management of significant process activities occurs at the process owner level.

The essential components of any measurement system are Critical Success Factors (CSFs) and Key Performance Indicators (KPIs).

2.5.2 Critical Success Factors with Key Performance Indicators

CSFs are defined as process- or service-specific goals that must be achieved if a process (or IT service) is to succeed. KPIs are the metrics used to measure service performance or progress toward stated goals.

The following CSFs and KPIs can be used to judge the efficiency and effectiveness of the process. Results of the analysis provide input to improvement programs (i.e., continual service improvement).

Table 3 describes the metrics that will be monitored, measured, and analyzed:

Table 3. ChM Critical Success Factors with Key Performance Indicators

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Changes are processed in a timely manner	1	RFC aging Calculation: Average number of days between RFC submission and RFC decision dates	Determines the timeliness and efficiency of the Change Management process by reviewing number of open changes and the length of time required before an RFC is decisioned
		2	RFC backlog/aging Calculation: Number of RFCs opened in previous reporting period and not yet decisioned	
2	Change process compliance by USMC IT and user communities is high	3	% of rejected RFCs Calculation: Percentage of RFCs closed in a rejected status	Determines the effectiveness of the process by demonstrating the number of rejected RFCs, tracking the trends in the monthly RFC totals, and demonstrates the level of
		4	Total number of RFCs opened	

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
			Calculation: Total number of RFCs opened in a one month period	adoption throughout the enterprise via the number of changes made outside the process
		5	Unauthorized changes Calculation: Number of discovered, unauthorized changes (i.e., changes that were implemented outside the ChM process)	
3	Production services are protected from the adverse impacts of change	6	% of authorized changes that result in an incident Calculation: % of RFCs linked to an incident record created after the RFC implementation date	Measure the primary objective of the ChM process by indicating the number of changes that result in incidents (i.e., self-imposed disruptions to service)

3.0 ROLES AND RESPONSIBILITIES

Each process has roles and responsibilities associated with design, development, execution and management of the process. A role within a process is defined as a set of responsibilities. Process Managers report process deviations and recommended corrective action to the respective process owner.

Management (i.e., responsibility) of a process may be shared; generally, a single enterprise process manager exists at the MCNOSC and at each MITSC. For certain processes, especially those within Service Design and Service Transition, managers also exist within MARCORSYSCOM and Programs of Record. Some Service Operation processes (e.g., Event Management) require managers at the RNOSC. There are instances where roles are combined or a person is responsible for multiple roles. Factors such as AOR, size of user base and size of the process support team dictate exactly which roles require a dedicated person(s) and the total number of persons performing each role. This process guide defines all *mandatory* roles.

3.1 Roles

The following abstract drawing depicts process roles for the USMC, followed by a description of these roles. **Note**: these are *roles* and not, necessarily, *billets.* One billet may cover multiple roles in accordance with the amount of work required within a particular Command, Region, or Enterprise level.

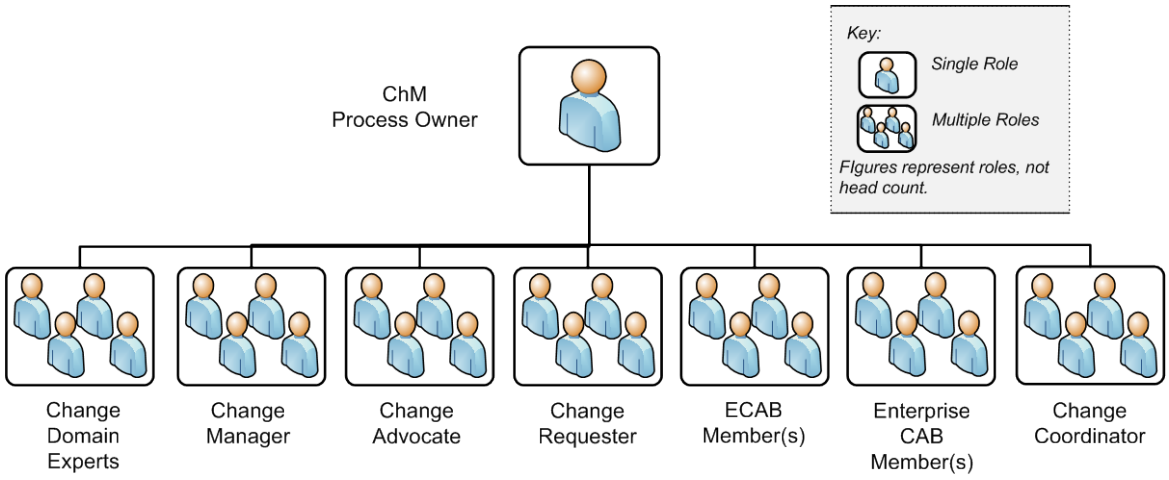


Figure 7. ChM Roles

The Enterprise Change Management Process owner is responsible for ensuring the process is fit for purpose. Responsibilities to include sponsorship, design, change management, and continual improvement of the process and its metrics. Multiple Change Managers exist at the regional (MITSC, RNOSC) and local levels. Where an RNOSC is co-located with a MITSC, it is expected the Change Manager covers both RNOSC and MITSC. Local commands, EITCs, and individual PORs have designated Change Managers (e.g., MCEITS SIE). These managers report upward, and receive policy guidance from, the Enterprise Change Management process owner.

Table 4. ChM Defined Roles and Responsibilities

Role	Overall Responsibility
Role #1 ChM Process Owner	
The Process Owner owns the process and the supporting documentation for the process. The primary functions of the Process Owner are oversight and continuous process improvement. To these ends, the Process Owner oversees the process, ensuring that the process is followed by the organization. When the process is not being followed or is not working well, the Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. In addition, the Process Owner is responsible for the approval of proposed changes to the process, and development of process improvement plans. May delegate specific responsibilities to another individual within their span of control, but remains ultimately accountable for the results of the ChM process.	Ensures that the Change Management process is fit for purpose Utilizes process performance metrics for analysis and identification of continual process improvement opportunities Endorse improvements to the process Ensures that all stakeholders are sufficiently involved in the Change Management process Ensures tight linkage between Change Management processes and other related processes Ensures that the process is defined, documented, maintained, communicated and users are trained Ensures organizational adherence to the process Ensures communication of the process roles and responsibilities Ensures the requirements for the Change Management system/tool are defined and secures the appropriate funding Ensures communication of the process performance metrics to stakeholders Ensures the process documentation complies to the organization's document control process
Role #2 Change Domain Expert (CDE)	
Recognized Subject Matter Expert (SME). Invited to CAB reviews when RFC falls within individual's expertise.	Provides comprehensive and accurate information for inclusion in RFC records Provides specialized skills and knowledge of one or more domains (technical, business, and/or application) to assist in the evaluation of the risk and impact of an RFC Involved in performing root cause analysis on failed changes Identifies and documents corrective actions for failed changes

Role	Overall Responsibility
Role #3 Change Manager	
Responsible for the daily execution of the ChM process, including the coordination of reviews, reporting, and scheduling.	Change Classification — Analyzes and seeks to understand change integration across the environment — Ensures that RFCs that do not meet the defined requirements are rejected Change Advisory Board (CAB) — Reviews all outstanding RFCs awaiting consideration or action — Facilitates the CAB meetings — Ensures management and customers are sufficiently informed as to schedule, impact, and cost of changes — Ensures that the CAB(s) are chartered and include(s) defined representation requirements — Decides on the composition of the CABs, and who is involved in assessing and validating the Change schedule based on charter Change Scheduling — Schedules all required non-emergency RFCs for CAB authorization, issues agendas and circulates all RFCs to CAB members in advance of authorization/meetings to allow prior consideration — Ensures communication of the Change Schedule (CS) across the organization — Ensures the Change Schedule (CS) is updated when required and published Change Implementation — Raises Change-related issues to the required level of management — Ensures that all RFCs are closed Post-Implementation — Reviews all implemented changes (post-change reviews) — Analyzes change records to detect any positive trends or problems and proposes actions to rectify apparent weak areas in the Change Management process

Role	Overall Responsibility
Role #4 Change Advocate	
Oversees and guides the RFC through the ChM process; aligned with the Change Requester.	Responsible for the shepherding of a specific change (as submitted by a Change Requester) throughout the ChM process Considers input from the Change Requester when assigning the initial priority, risk, and impact based on predefined change priority criteria Follows the Change Management process for building, testing, and implementing a change Provides additional information regarding the change when requested by the Change Manager Communicates change status to the IT Service stakeholders. Participates in the Post-Implementation Review process May recommend closure of assigned RFCs **Note:** Not all changes require a seperate Change Advocate. For small and/or emergency changes, the Change Advocate and Change Requestor are often the same person.
Role #5 Change Requester	
Initially submits a service request, triggering the ChM process.	Follows the Change Management process for submitting a service request In liaison with the Change Advocate, provides a clear description of the business needs, goals, and objectives of the requested change Provides additional information regarding the change when requested by the Change Manager Confirms the completed change can be closed after notification that the work has been completed Participates in the Post-Change Review and/or Post Implementation Review if requested
Role #6 Emergency Change Advisory Board (ECAB) Member	
ECAB member supports the assessment, prioritization, authorization, and scheduling of emergency changes.	Validates the emergency change is truly an emergency (based on emergency change criteria) Ensures RFC for Emergency Change receives appropriate authorization (based on ChM Policy) Makes the final decision that the resolution proposed to correct the production issue is the best option given the situation Ensures Emergency Change is reviewed by the CAB after implementation The ECAB consists of a change approver(s) according to the change approval matrix for each change model

Role	Overall Responsibility
Role #7 Change Advisory Board (CAB) Member	
CAB member supports the assessment, prioritization, authorization, and scheduling of changes.	Attends all relevant CAB meetings as required by the Change Manager Reviews all submitted Major and Significant RFCs to validate: — Their impact — Resources required to implement thema — Any ongoing costs — Adequate Planning — Implementation Readiness — Testing and Back-out Plans — Training — Schedule — Adequate communication with customers regarding downtime Provides decision upon review, or requests more information Participates in scheduling and coordination of the Forward Schedule of Changes When requested, participates in Change Post-Implementation Reviews
Role #8 Change Coordinator	
Acts as a liaison between the process and stakeholders as directed by the Change Manager.	Ensures RFCs submitted are valid, complete, and accurate Recommends to the Change Manager, rejection of any RFC that does not meet the defined criteria Raises Change-related issues to the required level of management Participates in other ITSM process initiatives and process reviews deemed necessary by the Change Manager

3.2 Responsibilities

Processes may span departmental boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The process owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Supporting, Consulted, Informed, Participant (RASCI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks.

Responsible – Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the 'A'.

Accountable – Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task.

Support – Resources allocated to support Responsible. Support helps complete the task

Consulted – Gives needed input about the process or activity. Prior to final decision or action, these subject matter experts or stakeholders are consulted.

Informed – Needs to be informed after a decision or action is taken. May be required to take action as a result of the outcome. This is a one-way communication.

Table 5 establishes responsibilities for high-level process activities by organization for the enterprise ChM process. Note that subordinate organizations (Regional and Local) have their own RASCI charts, which align with the enterprise.

*Table 5. Organizational Responsibilities for Enterprise ChM**

ChM Process Activities	MCNOSC	HQMC (C4)	MCSC (POR)	MCCDC	RNOSC	MITSC	Application Owner	Tenant/Supported Command
Initiate RFC	RA	S	S	S	CS	S	CS	CS
Create and Record RFC	RA	I	S			S	CS	
Assess RFC	RA		CS		CS	S	CS	
Authorize RFC	RA		CS		CS	S	CS	
Approve Schedule and Deployment	RA	I	S	I	CS	S	CS	I
Coordinate Deployment	RA	I	S	I	SC	SC	CS	I
Review and Close Change	RA	I	I		CS	CS	CS	

Legend:
Responsible (R) – Completes the process or activity, or who ensure that it is done as per Accountable
Accountable (A) – Authority to approve or disapprove the process or activity
Support (S) – Resources allocated to Responsible. Support helps complete the task
Consulted (C) – Experts who provide input
Informed (I) – Notified of activities

Note: Any department that is designated as Responsible, Accountable, Consulted, or Support is not additionally designated as Informed because being designated as Responsible, Accountable, Consulted, or Support already implies being in an Informed status. A department is designated as Informed only if that department is not designated as having any of the other four responsibilities.

Note: Only one department can be accountable for each process activity.

*This RASCI chart depicts responsibilities (only) for *enterprise* changes.

*Table 6. Role-Based Responsibilities for Enterprise ChM**

ChM Process Activities	Chm Process Owner	ChM Process Manager	ChM Process Coordinators	Change Domain Experts	Change Advocate	Change Requestor	Change Authority	Enterprise CAB Member	Emergency CAB Member
Initiate RFC	A			C	C	R			
Create and Record RFC	A	S	S	C	C	R			
Assess RFC	A	R	S	C		C	I		
Authorize RFC	A	S	S	C	I	I	R	S	S
Approve Schedule and Deployment	A	S	S	C	C	C	R	S	S
Coordinate Deployment	A	R	S	C	S				
Review and Close Change	A	R	S	S	C	C	I	I	I

Legend:
Responsible (R) – Completes the process or activity, or who ensure that it is done as per Accountable
Accountable (A) – Authority to approve or disapprove the process or activity
Support (S) – Resources allocated to Responsible. Support helps complete the task
Consulted (C) – Experts who provide input
Informed (I) – Notified of activities

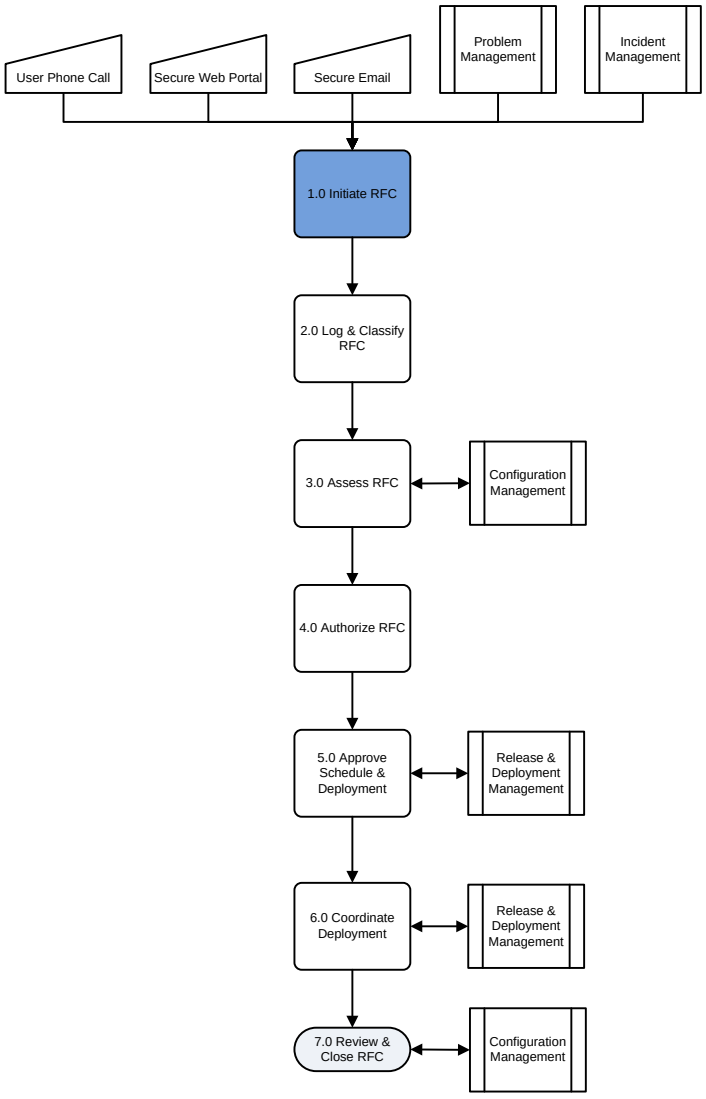
Note: Any department that is designated as Responsible, Accountable, Consulted, or Support is not additionally designated as Informed because being designated as Responsible, Accountable, Consulted, or Support already implies being in an Informed status. A department is designated as Informed only if that department is not designated as having any of the other four responsibilities.

Note: Only one role can be accountable for each process activity.

4.0 SUB-PROCESSES

The USMC ChM process consists of seven (7) sub-processes. These Level C processes (or activities) are described below, and remain relevant to the structure and activities adopted at the regional and local levels.

4.1 Initiate RFC



Change requests enter the process from multiple sources and through integration points with related processes, such as Incident Management and Problem Management. Change requests are initiated through the creation of a Change record within the Change Management tool.

A determination is made by the requestor using existing criteria on whether or not the request is for an emergency change. If it is, then the request is managed through the Emergency Change Procedure. If it is for a normal change, then the request is managed as follows.

There are two methods for the initiation of normal change requests. The first is through the direct creation of a RFC for proposed changes to the Operational baseline.

The second is through interaction with Service Portfolio Management for creation of a change proposal. Service Portfolio Management provides an initial decision on the change proposal through the Enterprise Service Request Validation Group. If the request is approved, then a RFC is created. Once initiated, the RFC proceeds to Logging and Classification.

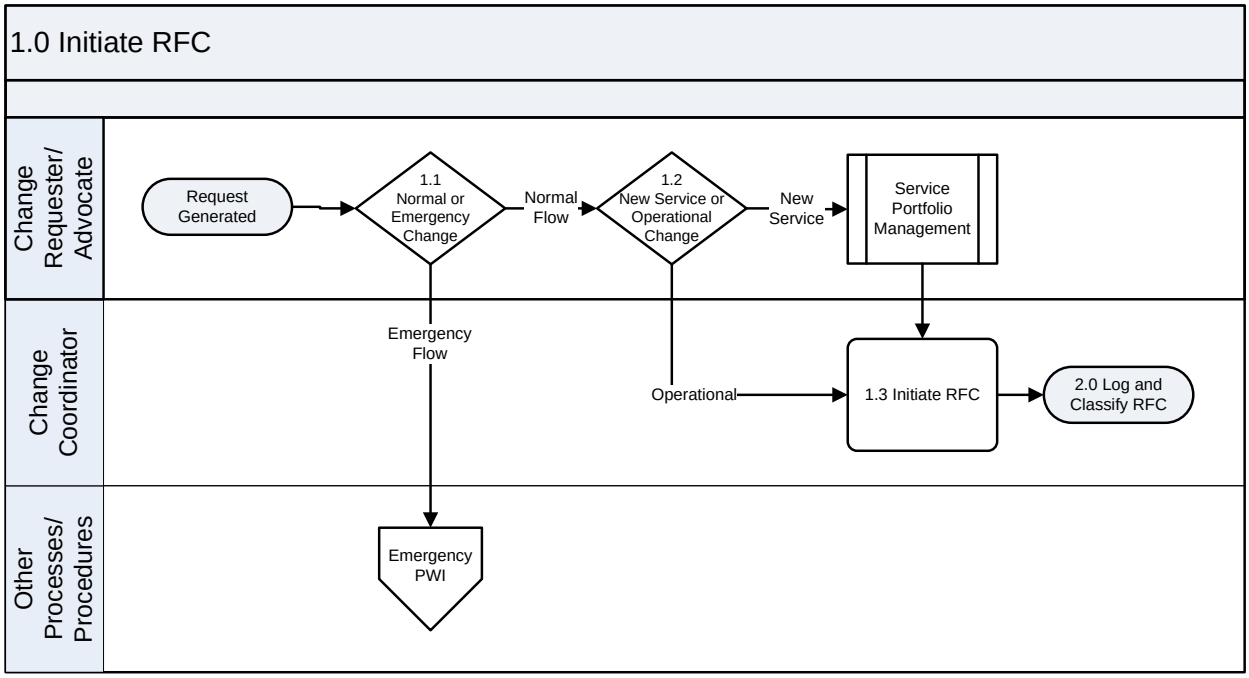


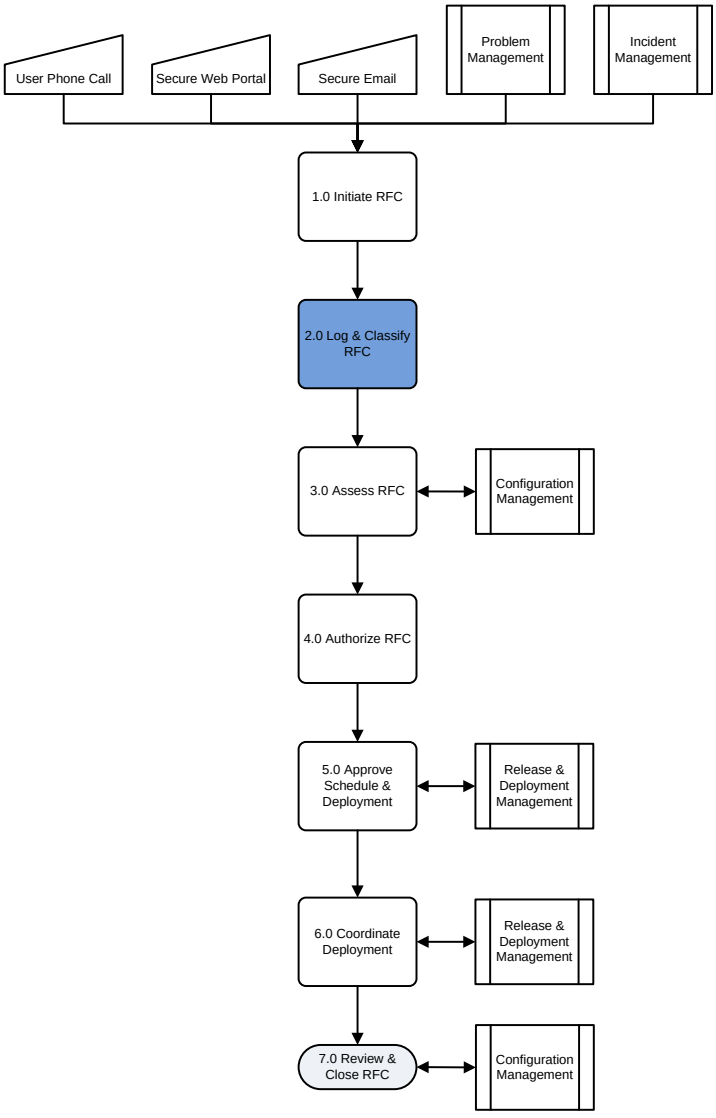
Figure 8: ChM Initiate RFC Sub-Process

Table 7. describes the Initiate RFC sub-process steps as depicted above in Figure 8:

Table 7. ChM Initiate RFC Sub-Process Descriptions

1.0 Initiate RFC		
Number	**Process Activity**	**Description**
1.1	Normal or Emergency Change	• The change requestor and/or advocate determines if the requested enterprise change is a normal or emergency change o If Enterprise Normal, then proceed to determining if the request is for a New Service or Operational Change. o If Enterprise Emergency, then create RFC as defined in the Emergency Procedure.
1.2	New Service or Operational Change	• The change requestor and/or advocate determines if the requested enterprise change is a new service or operational change o If New Service, then create Service Request for new or modified Service to be handled by Service Portfolio Management (SPM)*. o If Operational, then create RFC for an enterprise operational change. * ***Note****: SPM provides an initial decision on the validity of the request and if approved then routes the request for ChM to initiate the RFC. If SPM does not approve the request then that process closes it and informs the requestor.*
1.3	Initiate RFC	• SPM provides approval for the initial request and the Change Coordinator initiates the RFC. The RFC is then Logged and Classified.

4.2 Log & Classify RFC



The objectives of the *Log & Classify RFC* activity are:

To enable the proper logging of a valid (accepted) RFC.

To evaluate and classify the RFC against defined criteria and, when appropriate, to return incomplete or invalid RFCs to the initiator.

The *Log & Classify RFC* activity begins with the acceptance of a user-initiated RFC (see *1.0 Initiate RFC*). RFCs can be concerned with any part of the infrastructure or with any service or activity. RFCs within the scope of the Enterprise ChM process are those changes that affect CIs defined within the enterprise Configuration Management Plan (CMP).

Incomplete, inaccurate, or non-applicable (e.g., out of scope or non-enterprise) submissions are returned to the user or originating body with rationale.

There are the following types of changes:

- Normal Change: Any alteration to the production IT environment or any planned action that may cause an interruption of IT Services. Normal Changes require formal ChM control, review, and authorization, and they follow the standard ChM process activities.
- Emergency Change: A change that must be introduced as soon as possible. For example, to resolve or avoid a Major Incident that has high impact or severe degradation on the operation of the MCEN, or a priority security event such as implementing a security patch that is vital to the mission effectiveness of deployed and contingency USMC forces. An Emergency Change must be implemented within a timeframe that does not allow normal change review; therefore Emergency Changes follow a condensed Normal Change process. Emergency changes are submitted to the ECAB for authorization or rejection. The ECAB is a sub-set of the CAB that makes decisions about Emergency Changes.

Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.

NOTE: Each RFC is reviewed for its particular circumstances. A Critical or High Priority value, or a high Risk value does not necessarily mean that a change is an emergency.

- Standard Changes: A common change to a service or infrastructure that is low-risk, low-cost, and has a proven and well-documented implementation plan. A Standard Change requires pre-authorization by ChM and the CAB, but once authorized they do not require case-by-case CAB approval. Standard Changes are still logged and tracked but may use a different mechanism, such as a Service Request. Standard Change examples:
  - Password change
  - Upgrade of a Personal Computer (PC)
  - Desktop move for a single user

Operational changes are assigned a priority classification based on the result of the Change Management *Impact*, *Urgency* and *Priority* system. Strategic service design changes are prioritized separately by Program Management.

- Impact is defined as the measure of the effect of a change on the USMC's mission, services, and systems.
- Urgency of a change is based on how long the implementation can afford to be delayed (to resolve a situation or fulfill a need).
- Priority is the result of Impact and Urgency and denotes the classification (i.e., *Critical*, *High*, *Medium*, or *Low*) and relative importance of a change (its Priority) as compared to other changes.

The *Impact* and *Urgency* system is shown in Figure 9 below, with its resulting *Priority* classification (*Critical*, *High*, *Medium*, or *Low).*

URGENCY	IMPACT			
	1 – Extensive / Widespread	2 – Significant / Larger	3 – Moderate / Limited	4 – Minor / Localized
1 – Critical	Critical	Critical	High	High
2 – High	Critical	High	High	Medium
3 – Medium	High	Medium	Medium	Medium
4 – Low	Low	Low	Low	Low

Figure 9: ChM Impact and Urgency Classification System

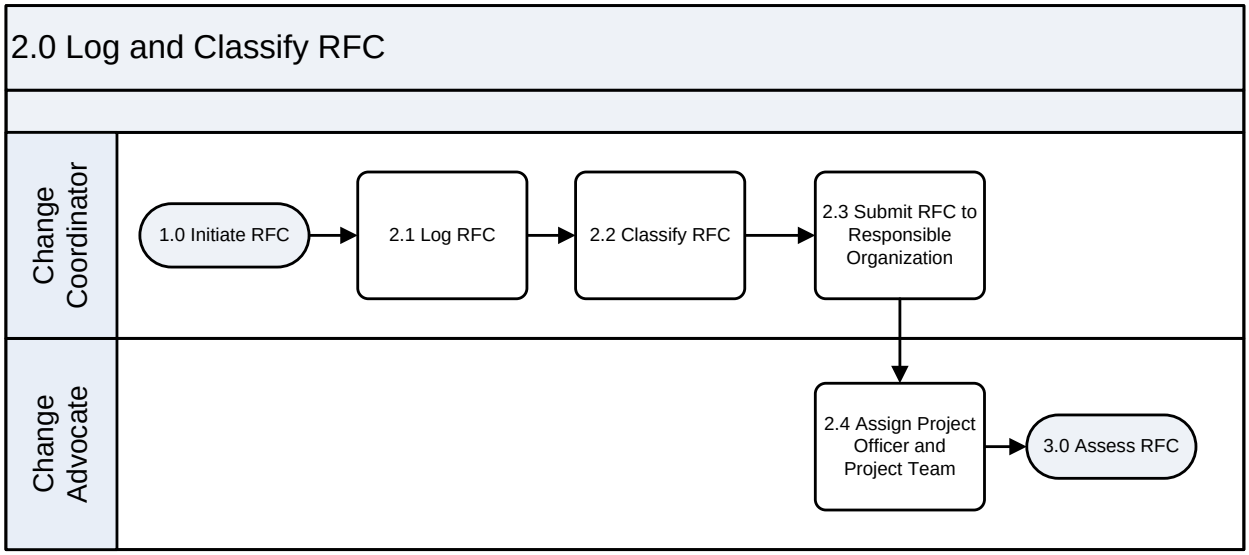


Figure 10: ChM Log and Classify RFC Sub-Process

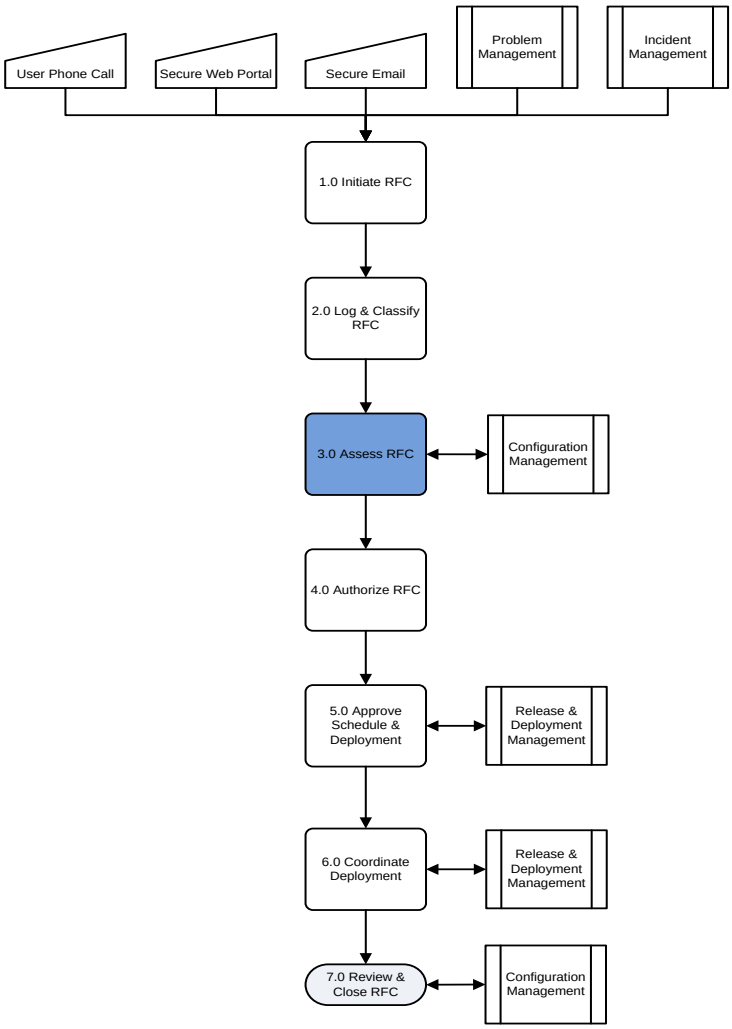
Table 8 describes the Log and Classify RFC sub-process steps as depicted above in Figure 10:

Table 8. ChM Log and Classify RFC Sub-Process Descriptions

2.0 Log and Classify RFC		
Number	**Process Activity**	**Description**
2.1	Log RFC	• Provide an RFC summary and detailed notes. • Provide RFC miscellaneous details (e.g., information about the RFC requester; the IT Service(s) affected by the change; the action to be taken, and the equipment, software, or systems that the action is to be taken against, etc.). Provide required information based on the

2.0 Log and Classify RFC		
Number	**Process Activity**	**Description**
		Change Model (e.g., Back-Out Plan, Deployment Plan). • Associate known CIs to the RFC. • Request a schedule for deployment of the RFC .
2.2	Classify RFC	• Classify RFC based on impacted service/functional area for assignment to a responsible organization. Ensure inclusion of the initial Business Case Analysis which will contain the technical impact, the impacted IT services, mission impact, financial and resource impact, risk analysis, and initial schedule and deployment requirement.
2.3	Submit RFC to Responsible Organization	Submit the RFC to the responsible organization for the type of request as determined by the Functional Area matrix.
2.4	Assign Project Officer and Project Team	The Responsible Organization assigns a project officer and resources as required for project support. Resource may include, but not limited to: Engineering Technical Lead, Technical Authority, etc.

4.3 Assess RFC



The objectives of the *Assess RFC* activity are:

To validate RFC (completion, accuracy, classification, etc.)

To determine the level of review required for deciding the RFC (including whether external review processes/authorities are required)

The *Assess RFC* activity analyzes each RFC to determine its impact on existing and planned CIs as well as the impact on resources required to build and deploy the change.

The urgency required for change implementation is assessed. When combined with the mission impact, changes are assigned a priority. Additional factors influence change prioritization, including financial, contract, certification, and security requirements. These factors are reviewed by the appropriate functional representation.

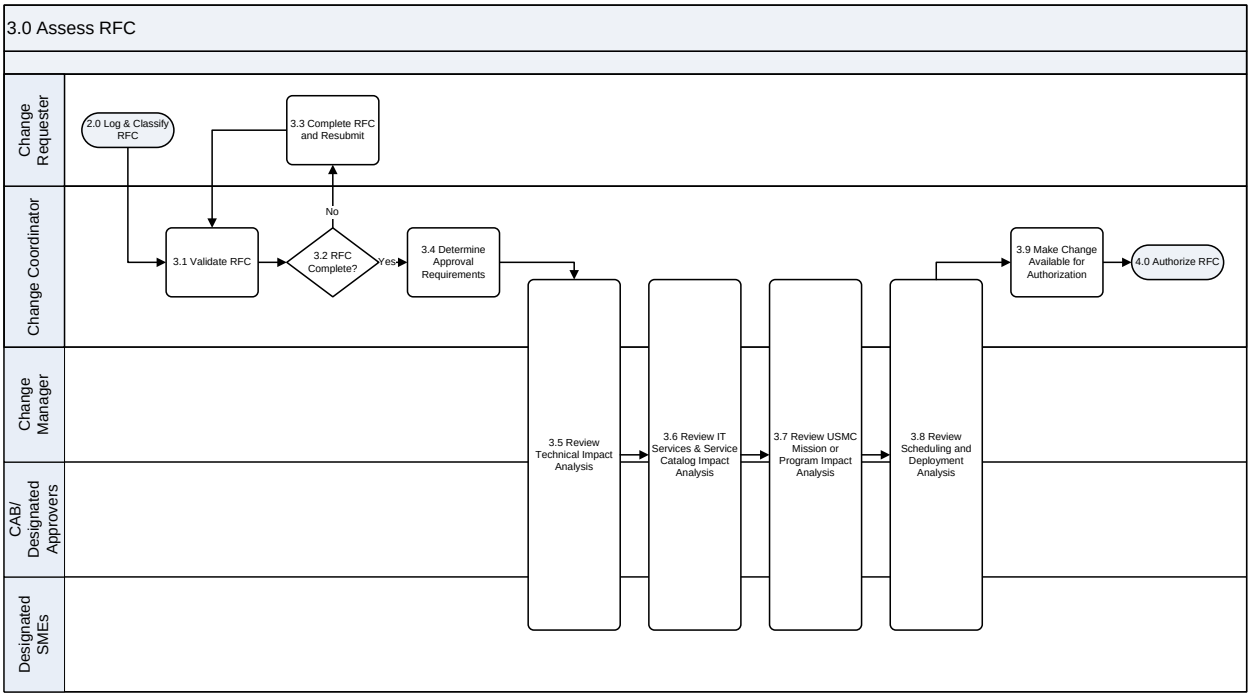


Figure 11. ChM Assess RFC Sub-Process

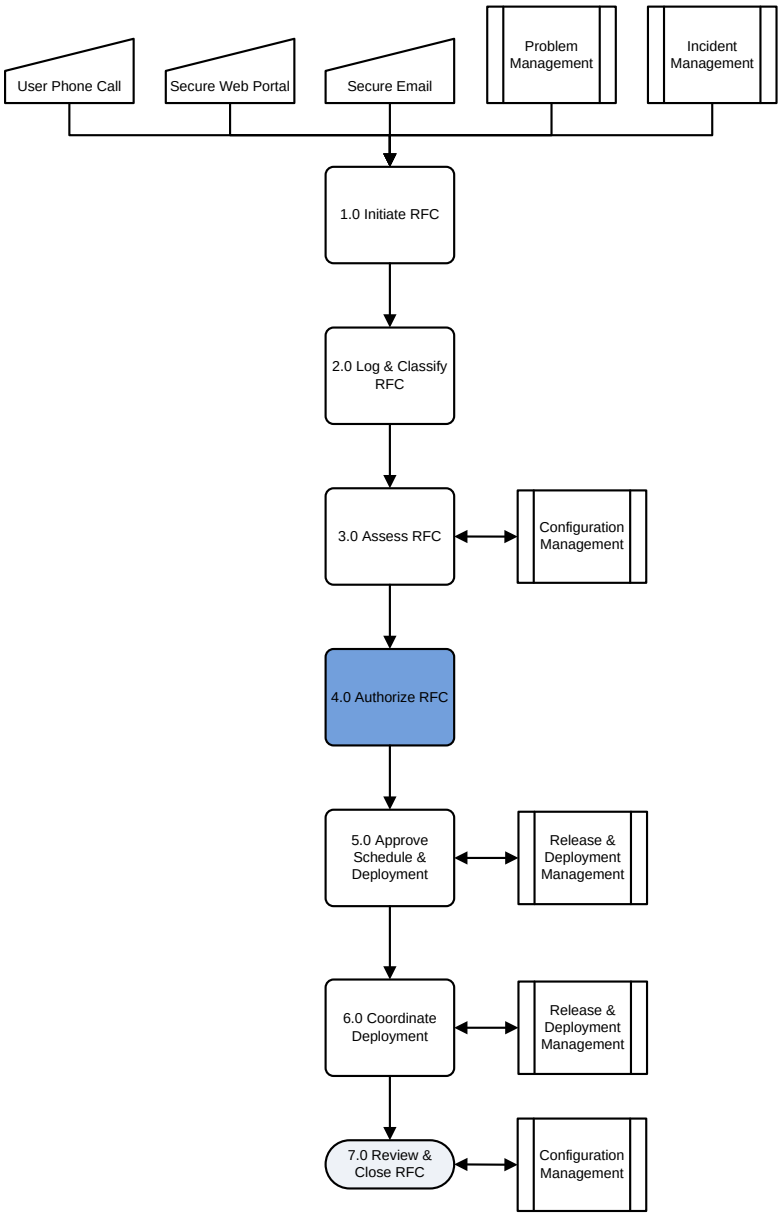
Table 9 describes the Assess RFC sub-process steps as depicted above in Figure 11:

Table 9. ChM Assess RFC Sub-Process Descriptions

3.0 Assess Change		
Number	**Process Activity**	**Description**
3.1	Validate RFC	Determine if accurate change model (e.g., minor, standard, major) has been ascribed to the change via 2.0, *Log & Classify Change*. The Change Manager retains authority to modify classification and/or return the RFC to the Change Requester for further action.
3.2	RFC Complete?	
3.3	Complete RFC and Resubmit	If the RFC is determined to be incomplete by the Change Manager, the Change Advocate (working with Change Requester as required) reviews the information required to complete the RFC, performs the requested actions to complete the RFC, and re-submits the RFC for validation. If the RFC is determined to be complete, it progresses to step 3.4, *Determine Approval Requirements.*
3.4	Determine Approval Requirements	Determine the persons and/or organizations that must review the change. Determine composition of the CAB.Determine appropriate Change Authority.
3.5	Review Technical Impact Analysis	Designated evaluators assess the impact and risk of the proposed change to relevant technical operations. Evaluators also assess the impact and risk of *not* implementing the change, especially if the change is to fix or improve existing technical operations of infrastructure components.
3.6	Review IT Services and Service	Designated evaluators assess the impact and risk to IT

3.0 Assess Change		
Number	**Process Activity**	**Description**
	Catalog Impact Analysis	Services and the Service Catalog structure and content.
3.7	Review USMC Mission or Program Impact Analysis	Designated evaluators assess the impact and risk of the proposed change to USMC operations or program schedules/cost. Evaluators also assess the impact of *not* implementing the change, especially if the change is to fix or improve existing mission or program activities.
3.8	Review Scheduling and Deployment Analysis	Designated evaluators review the Change Calendar (contains information about all the upcoming changes and their implementation dates), deployment approach (e.g., how the RFC will be deployed within deployment windows and the recommended number of RFCs), required resources (e.g., personnel, equipment), and projected service availability impact, including impact on SLAs (where available).
3.9	Make Change Available for Authorization	Pertinent information on the change is tailored to the respective reviewing body (e.g., technical information for the technical assessment team) and forwarded accordingly.

4.4 Authorize RFC



Authorize RFC obtainsfinal authorization by the change authority.

The objectives of this activity are:

Review the RFC and accompanying information for purposes of deciding the RFC

Change Authority authorizes, requests additional information, or rejects RFC.

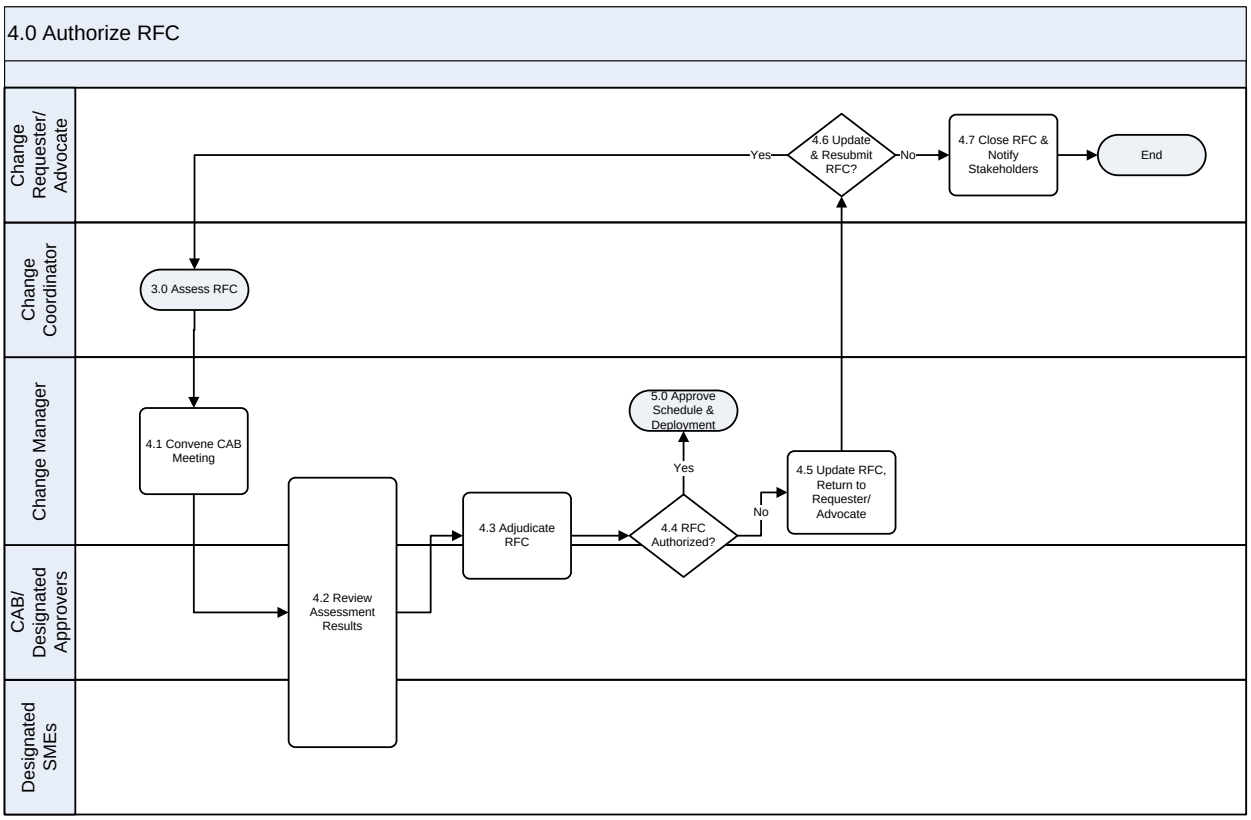


Figure 12. ChM Authorize RFC Sub-Process

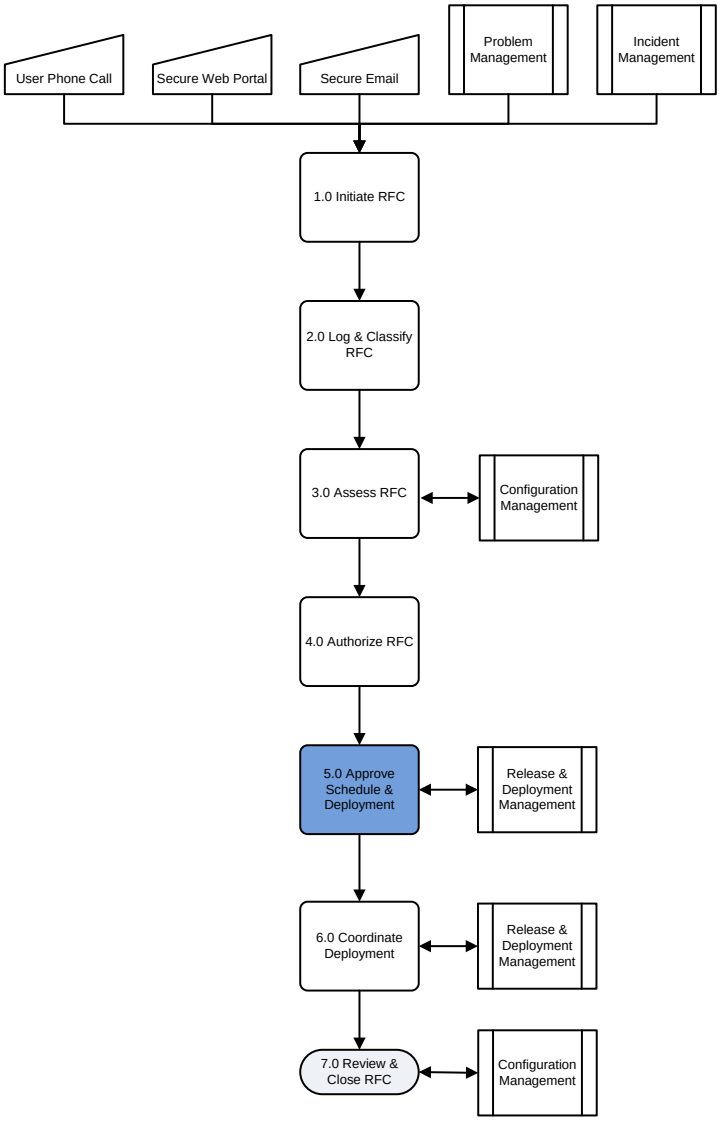
Description of the Authorize RFC workflow sub-process is given in Table 10.

Table 10. ChM Authorize RFC Sub-Process Descriptions

4.0 Authorize RFC		
Number	**Process Activity**	**Description**
4.1	Convene CAB Meeting	The CAB meets to review and provide advice on submitted RFCs.
4.2	Review Assessment Results	Conduct review of collected business, program, and/or technical impact assessments. Determine urgency of the change. Prepare information for eventual review by the change authority (e.g., EntCAB). Ensure that required RDM involvement is coordinated with the appropriate RDM Manager.
4.3	Adjudicate RFC	The change authority, as determined based on the type of the RFC, adjudicates the RFC (see 2.3.1.2).
4.4	RFC Authorized?	Authorized RFCs progress to the next activity, *Approve Schedule and Deployment.* ***Note**: Authorized RFCs are subject to deployment review (by ChM and/or RDM) and are not automatically approved for implementation.*
4.5	Update RFC, Return to Requester/Advocate	Returned RFCs are updated with the rationale, such as incomplete data, lack of funding, ambiguous or unknown benefits of change implementation, etc..

4.0 Authorize RFC		
Number	**Process Activity**	**Description**
		Rejected RFCs are returned to the Change Advocate/Change Requester with the accompanying rationale and closed.
4.6	Update and Resubmit RFC?	The Change Requester and/or Change Advocate retain the ability to modify returned RFCs based upon feedback and re-submit, provided noted discrepancies have been properly addressed.
4.7	Close RFC and Notify Stakeholders	RFCs placed in a final state (*Rejected*, *Cancelled*, or *Closed*) must be communicated to the stakeholders.

4.5 Approve Schedule and Deployment



The objective of this activity is to finalize scheduling and approve deployment of authorized changes and ensure such changes remain aligned with mission needs. ChM confers with RDM on planning the release (requirements, duration, resources, etc.) and incorporating the change into a release package. RDM oversees testing the release package according to the approved test plans (including tests of the Implementation Plan, the Back-out Plan, etc.). ChM receives the results of the testing from RDM; this includes issues, risks, recommendations and action plans. Unsuccessful testing can mean the RFC needs additional work and needs to go through the 4.0 Authorize RFC process activities again for review and adjudication.

The Change Manager is responsible for deconflicting Change Schedules, and publishing the schedule accordingly. The result is an updated Change Schedule, containing details of all approved changes and their implementation dates, projected service outages, containing details of changes to agreed Service-Level Agreements (where available) and service availability.

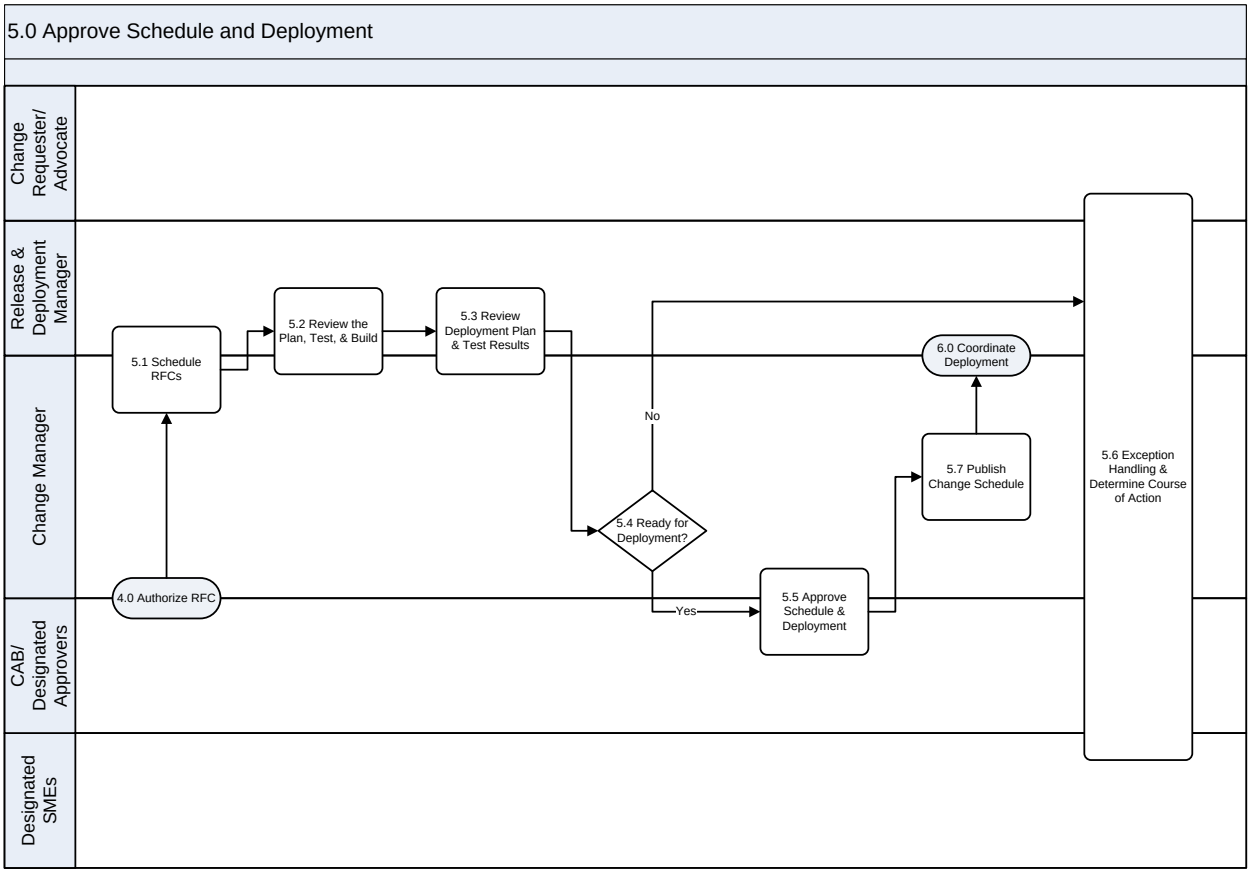


Figure 13. ChM Approve Schedule and Deployment Sub-Process

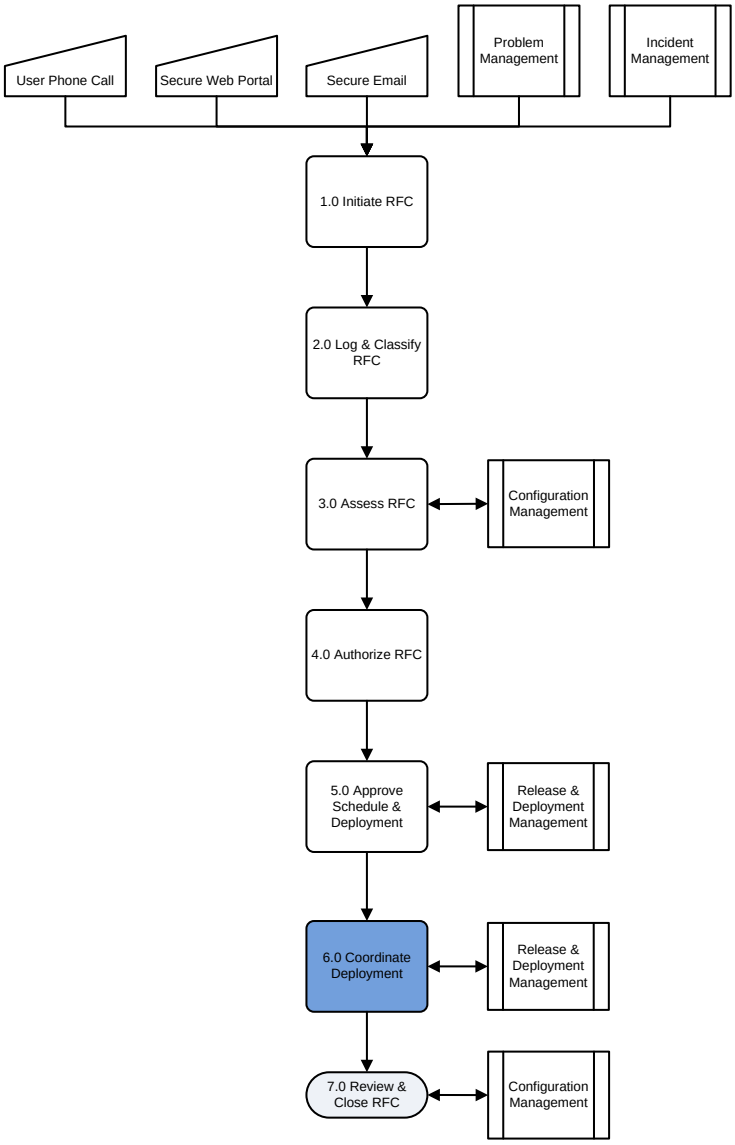
Description of the Approve Schedule and Deployment workflow sub-process is given in Table 11.

Table 11. ChM Approve Schedule and Deployment Sub-Process Descriptions

5.0 Approve Schedule and Deployment		
Number	**Process Activity**	**Description**
5.1	Schedule RFCs	ChM and RDM schedule RFCs that are "authorized but unscheduled" (i.e., RFCs that the designated authorizer(s) and CAB authorized but did not specifically schedule in *4.0 Authorize RFC*).
5.2	Review the Plan, Build, and Test	ChM confers with RDM and monitors and ensures that planning, building and testing of the release occurs according to the approved plans.
5.3	Review Implementation Plan and Test Results	RDM collates the results of testing – including the risks, mitigation and recommended exception handling – and reports the results to ChM, which in turn distributes to stakeholders.
5.4	Ready for Deployment?	Based on the test results ChM determines whether the RFC/Release is ready to deploy.
5.5	Approve Schedule and Deployment	The Change Authority approves the schedule for and deployment of the Release. Note: Where required, obtain concurrence from operational entities prior to deployment.

5.0 Approve Schedule and Deployment		
Number	**Process Activity**	**Description**
5.6	Exception Handling and Determine Course of Action	When it's determined that testing is not successful then ChM initiates exception handling with RDM and determines a course of action.
5.7	Publish Change Schedule	ChM publishes the Change Schedule which contains information about approved changes and their implementation dates.

4.6 Coordinate Deployment



Objectives of this activity include:

- To ensure that changes are implemented according to the approved release schedule
- To ensure that changes are implemented according to the approved Implementation Plan and Back-out Plan (if required)
- To ensure that service disruption to the customers of IT Services is minimized

Change Management maintains shared responsibility with RDM for ensuring that changes are implemented as scheduled. This role is largely one of coordination and collaboration as the actual implementation is the responsibility of RDM and designated technical experts. Authorized changes, with their scheduled implementation dates and milestones, are passed to RDM and the relevant technical groups.

The Change Manager receives and acts on notifications and status updates received from RDM. Updates from the deployment team may specify resolution action plans to solve any issues uncovered in the deployment with work-around activities to lessen service, application and user impacts.

If unrecoverable failures are encountered in the deployment, or if the release is at risk of breaching the approved deployment schedule, ChM may receive recommendations from RDM and the deployment team to initiate a back-out.

After the deployment is completed, RDM informs ChM on the result (i.e., successful or unsuccessful).

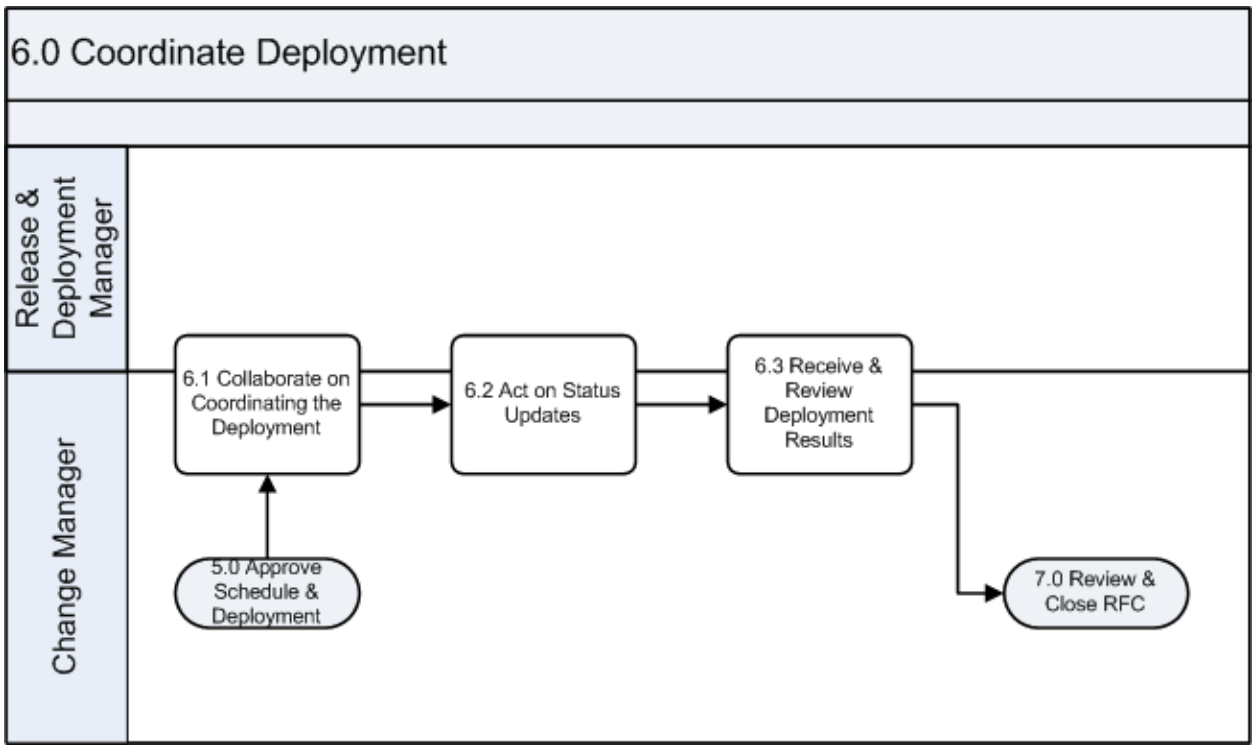


Figure 14. ChM Coordinate Deployment Sub-Process

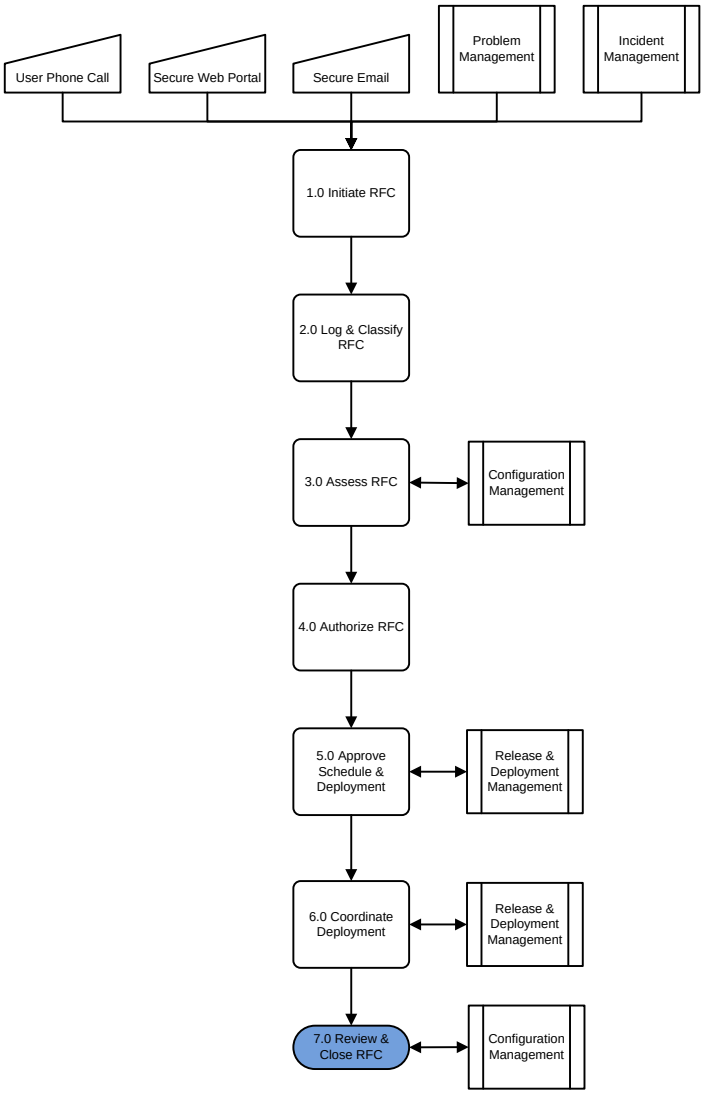
Description of the Coordinate Deployment workflow sub-process is given in Table 12.

Table 12. ChM Coordinate Deployment Sub-Process Descriptions

6.0 Coordinate Deployment		
Number	**Process Activity**	**Description**
6.1	Collaborate on Coordinating the Deployment	ChM and RDM collaborate on and maintain a shared responsibility in coordinating deployments. ChM and RDM ensure that: • RFCs are implemented according to the approved Test Plan(s), Implementation Plan, and Back-out Plan (as required). • RFCs are implemented according to the approved release schedule. • Service disruption to the customers of IT Services is minimized.
6.2	Act on Status Updates	ChM acts on status updates from RDM: • Notifications from RDM provide details about deployment accomplishments including the acceptance criteria met and the readiness status. Updates from the deployment team may specify resolution action plans to solve any issues uncovered in the deployment with work-around activities to lessen IT Service, application, and user impacts. • If unrecoverable failures are encountered in the deployment, or if the release is at risk of breaching the approved deployment schedule, ChM may receive recommendations to initiate a back-out.
6.3	Receive and Review Deployment	After the deployment RDM informs ChM about the

6.0 Coordinate Deployment		
Number	**Process Activity**	**Description**
	Results	deployment results (i.e., successful or unsuccessful.) • Successful deployments are progressed to completed status. • Deployments that are not successful are noted as such and the reason why is communicated to the RFC Requester and stakeholders.

4.7 Review and Close RFC



Objectives of this activity include:

Closing Change Records when change implementation is completed

Optimizing Change Management effectiveness and efficiency

Enabling continuous improvement of the ChM process

This activity describes the tasks involved in reviewing all implemented changes, after a predefined period has elapsed. It ensures that the Change has had the desired effect and met its objectives, and that Users and Customers are content with the results. The Review activity determines whether the Implementation Plan and/or the Back-out Plan worked correctly, and whether the Change was implemented on time and to cost. Additionally, the Change Manager validates RDM updated the CMDB with the configuration changes that occurred in the release. The Close activity determines whether any follow-up action (such as the creation of a new RFC) is required and if not, a formal close of the RFC is performed. The closure of an RFC includes updating other process areas of the status of the Change.

Any nonconformity should be recorded and actioned. Any weaknesses or deficiencies identified in a review of the change control process are fed into service improvement plans.

Where a Change has not achieved its objectives, ChM decides what follow-up action is required, which could involve raising a revised RFC. If the review is satisfactory or the original Change is abandoned, the RFC is formally closed in the logging system.

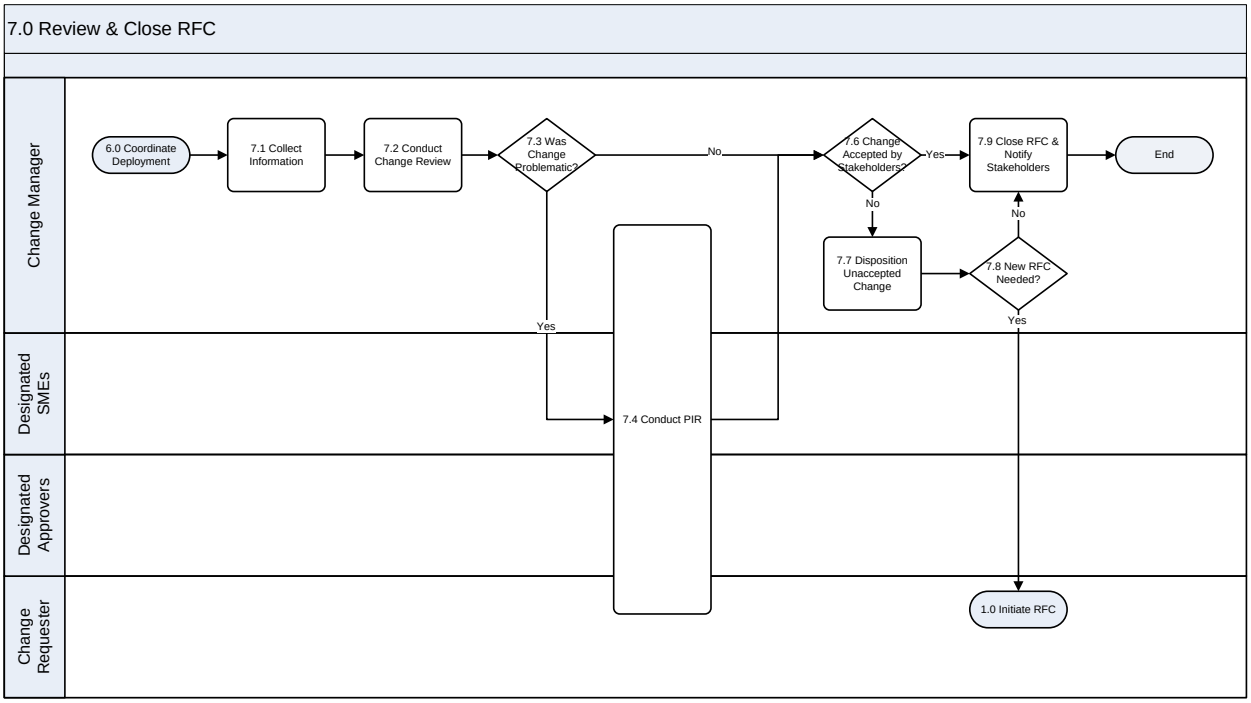


Figure 15. ChM Review and Close RFC Sub-Process

Table 13. ChM Review and Close RFC Sub-Process Descriptions

7.0 Review and Close RFC		
Number	**Process Activity**	**Description**
7.1	Collect Information	The Change Manager gathers all pertinent information to include any provided stakeholder feedback in preparation for subsequent review.
7.2	Conduct Change Review	ChM reviews all implemented Changes. The purpose of these reviews is to establish that: The Change has the desired effect and met its objectives Users and Customers (stakeholders) are content with the results, or any shortcomings are identified There have been no unexpected or undesirable side-effects to functionality, availability, capacity/performance, security, maintainability etc. The resources used to implement the Change were as planned The implementation plan worked correctly (include comments from the implementers) The Change was implemented on time and to cost The back-out plan functioned correctly, if needed
7.3	Change Built and Installed Correctly?	A problematic change (i.e., one not properly built or failing test activities) is always subject to Post Implementation Review (PIR).

7.0 Review and Close RFC		
Number	**Process Activity**	**Description**
7.4	Conduct PIR	A PIR is a formal change review activity that investigates problematic changes or any change as directed by the Change Manager. A PIR covers all aspects of a standard change review with a focus on root cause analysis and continual service improvement for the purposes of preventing future failed changes. All Emergency Changes shall go to PIR. Review board members are invited at the behest of the Change Manager and include, at a minimum, the technical subject matter experts and those persons involved in the initial authorization activity for the change in question. The Change Manager is responsible for ensuring any action items that result from PIR are effectively addressed and closed.
7.5	Change Accepted by Stakeholders?	Upon completion of a change and the change review or Post-Implementation Review process, stakeholders are notified of the implementation and any exceptional circumstances that may have arisen. Stakeholders retain the ability to indicate non-acceptance of changes post-deployment. If changes are accepted (by expressed approval or absence of stakeholder comment), the change progresses to close RFC and Notify Stakeholders.
7.6	Disposition Unaccepted Change	In the event stakeholders do not accept a change or the outcomes of a PIR, the Change Manager is responsible for communicating with unsatisfied stakeholders to ascertain the reasons for non-acceptance and the possible need and feasibility of a follow-on RFC initiation. If consensus and validation cannot be achieved, the disposition is escalated for action to the appropriate CAB.
7.7	New RFC Needed?	An RFC initiated as the result of this process is linked to the original RFC record; the new RFC follows the 1.0, *Initiate RFC* process, as documented.
7.8	Close RFC and Notify Stakeholders	The RFC is closed when it has been successfully implemented and accepted by involved stakeholders. Communication to stakeholders is via the Change Manager or designated representative.

Appendix A – ACRONYMS

The official list of E-ITSM acronyms can be found on the Enterprise Information Technology Service Management site (https://eis.usmc.mil/sites/irm/ITSM/default.aspx). The link to the document is referenced below:

https://eis.usmc.mil/sites/irm/ITSM/Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Firm%2FITSM%2FDocuments%2FE%2DITSM%20Acronym%20List&FolderCTID=0x0120001918760B7D35A5478C0474985E3ACBCD&View={9CD820B3-EF85-4D2C-BD0C-A255AEE9E40D}

Appendix B – GLOSSARY

Term	Definition
Asset Management	Asset Management is the process responsible for tracking and reporting the financial value and ownership of assets throughout their lifecycle.
Back-out Plan	A Back-out Plan is developed in the Release planning phase. This plan provides a recovery plan to return to the original configuration or process if the release fails to achieve the planned outcome.
Backup	Backup is copying data to protect against loss of integrity or availability of the original data.
Change Proposal	A high level description of a potential new service introduction or significant change to an existing service, along with a corresponding business case and a preliminary implementation schedule. If the change proposal is authorized, then Service Portfolio Management will charter the service.
Change Record	A record containing the details of a change. Each change record documents the lifecycle of a single change. A change record is created for every request for change that is received, even those that are subsequently rejected. Change records should reference the configuration items that are affected by the change. Change records will be stored in the Enterprise Change Management tool.
Change Request	See Request For Change
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
Configuration Control	Configuration Control is a sub-process of Configuration Management. Configuration Control is a set of processes and approval stages required to change a CI attribute. Configuration Control encompasses the oversight to ensure that a CI is changed through the Change Management process.
Configuration Identification	A sub-process of Configuration Management, Configuration Identification is the selection, identification, and labeling of the configuration structures and CIs including their respective technical owner and the relationships between them. CIs become the manageable unit that is planned for release into a configuration controlled environment. The CIs consist of hardware, software, services, and documentation.
Configuration Item	A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System (CMS) and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and SLAs.
CI Type	CI Type is a category used to Classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: server, document, user, etc.
Configuration Management Database	A Configuration Management Database (CMDB) is a database used to store configuration records throughout their lifecycle. The Configuration Management System (CMS) maintains one or more CMDBs and each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management Plan	Document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program. (Source: MIL HDBK-61A)
Configuration Management System	A Configuration Management System (CMS) is a set of tools and databases used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes, and releases and may contain data about employees, suppliers, locations, units, customers and users. The CMS includes tools for collecting, storing, managing, updating and presenting data about all CIs and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management processes.
Critical Succes Factor (CSF)	A condition that must be in place, or something that needs to happen, for the service or process to be considered successful.

Term	Definition
Deployment	Deployment is the activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment. Deployment is part of the Release and Deployment Management Process.
Deployment Readiness Test	A Deployment Readiness Test is conducted to ensure that the deployment processes, procedures, and systems can deploy, install, commission, and decommission the release package and resultant new or changed service in the production/deployment environment.
Deployment Verification Test	A Deployment Verification Test is conducted to ensure the service capability has been correctly deployed for each target deployment group or environment.
Early Life Support	Early Life Support (ELS) involves Technical Management or IT Operations providing support for a new or changed IT service for a period of time after it is released. During ELS, the IT service provider may review the KPIs, service levels, and monitoring thresholds and provide additional resources for incident management and problem management (when implemented).
EM System	The Event Management System (EMS) is comprised of tools which monitor CIs and provide event notifications. It is a combination of software and hardware which provides a means of delivering a message to a set of recipients. The EMS often requires real-time interaction, escalation, and scheduling.
Environment	Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something.
Error	An Error is a design flaw or malfunction that causes a failure of one or more CI or IT services. A mistake made by a person or a faulty process that affects a CI or IT service is also an error.
Escalation	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
Event	An Event is a piece of data that provides information about one or more system resources. Most events are benign. Some events show a change of state which has significance for the management of a CI or IT service. The term 'event' is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
Event Correlation	Event correlation involves associating multiple related events. Often, multiple events are generated as a result of the same infrastructure fault. Events need correlation to prevent duplication of effort in resolving the original fault.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Fault	Fault is the deviation from *normal* operation of a CI or a series of CIs. A fault is a design flaw or malfunction that causes a failure of one or more CIs or IT services. Fault is also referred to as an error.
Governance	Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring, and reporting and taking actions to resolve any issues identified.
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
Known Error	A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their lifecycle by Problem Management. Known errors may also be identified by vendors.

Term	Definition
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known.
Notification	Notification is a communication that provides information.
Pilot	A Pilot is a limited deployment of an IT service, a release, or a process to the live environment. A pilot is used to reduce risk and to gain user feedback and acceptance. They are of limited duration and removed at the conclusion of the pilot.
Procedure	See Standard Operating Procedure
Process	A Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Request for Change	A formal request for a change to be made. It includes details of the proposed change, and will be recorded in the Enterprise Change Management tool.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
	Remove reference in Sec 2.3.1
Service Design Package	A Service Design Package (SDP) is composed of document(s) defining all aspects of an IT service and its requirements through each stage of its lifecycle. An SDP is produced for each new IT service, major change, or IT service retirement.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.
Service Knowledge Management System	A Service Knowledge Management System (SKMS) is a set of tools and databases used to manage knowledge and information. The SKMS includes the Configuration Management System (CMS) as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT service provider needs to manage the full lifecycle of IT services.
Service Level Agreement	A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service, documents service-level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Service Validation and Testing	Service Validation and Testing is the process responsible for validation and testing of a new or changed IT service. Service Validation and Testing ensures an IT service matches the design specification and will meet the needs of the business. Service Validation and Testing during release conducts testing in the pre-production environment and during deployment in the pilot production environment.
Standard Operating Procedure	A set of instructions applicable to those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness.
Test	A Test is an activity that verifies that a CI, IT service, or process meets its expected results.
Test Environment	A Test Environment is a controlled environment used to test CIs, builds, IT services, and processes.
User Acceptance Testing	User Acceptance Testing is a testing activity conducted by the user intended to verify a CI, IT service, or process meets a requirement.
Work-around	Work-arounds for problems are documented in known error records and are intended to reduce or eliminate the impact of an incident or problem for which a full resolution is not yet available. Work-arounds for incidents that do not have associated problem records are proposed in the incident record.
Work Instruction	The Work Instruction is a document containing detailed instructions that specify exactly what steps are followed to carry out an activity. A work instruction is tool specific.